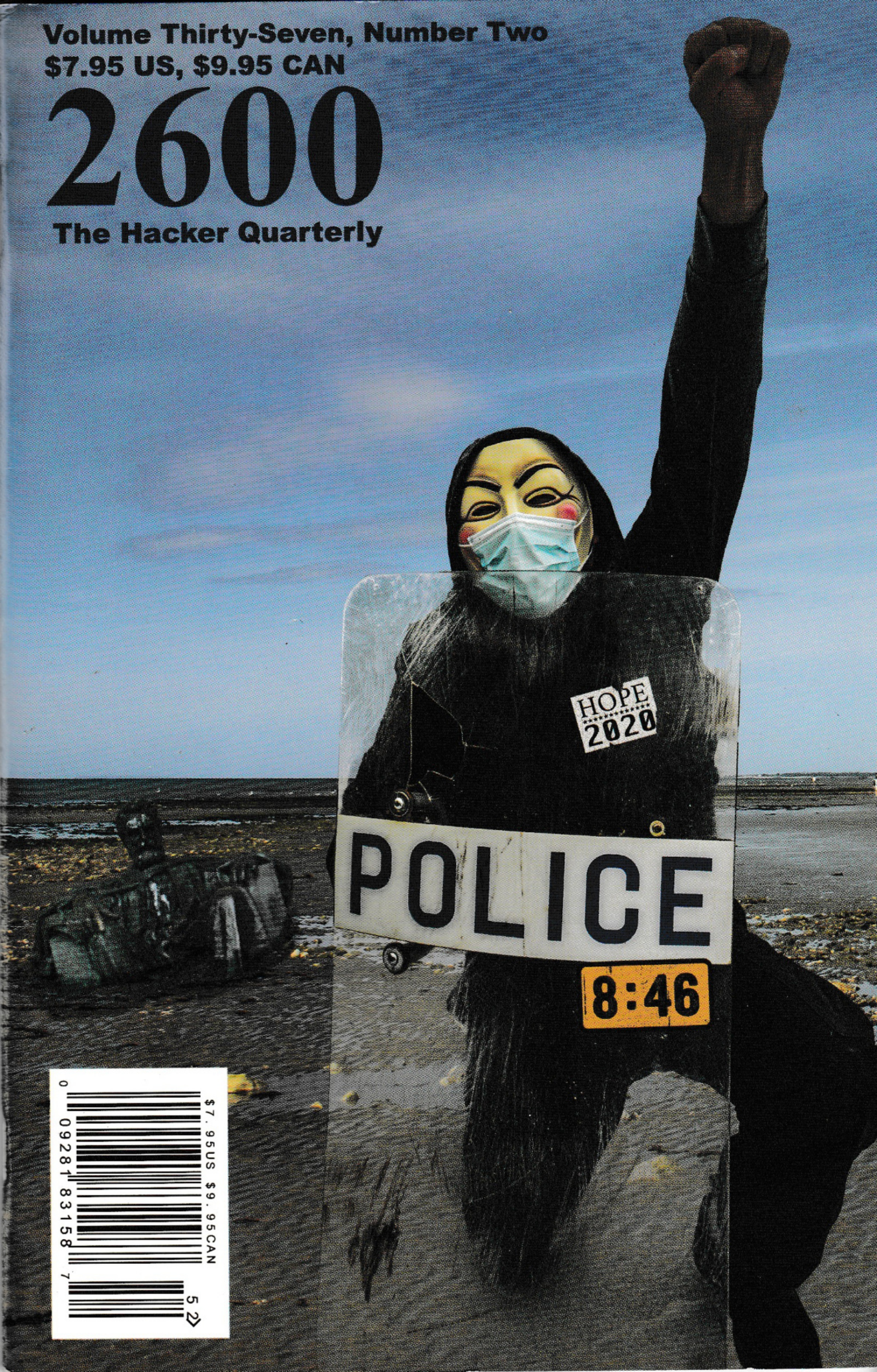
Volume Thirty-Seven, Number Two
$7.95 US, $9.95 CAN

2600

The Hacker Quarterly



0 09281 83158 7
$7.95US $9.95CAN
52

Mexican Payphones

Puerto Vallarta. Who says payphones can't find a use after people no longer seem to want to use them to make calls? This one somehow wound up on the ground and is doing quite nicely as a table.

Photo by Howard Cherniack

Nuevo León. Seen in the Zona Piel district, this phone is clearly treated with more respect than the post it's fastened to.

Photo by CG Brit

Guadalajara. This phone is still working and models like it can be found on streets all over. We're told the prepaid cards are nearly impossible to find, however....

Photo by Francisco Treviño

Mexico City. To be fair, this phone is located indoors, which is why it looks even more pristine than the others - although it's still possible it's rarely used.

Photo by Bret Miller

Got foreign payphone photos for us? Email them to payphones@2600.com. Use the highest quality settings on your digital camera! (Do not send us links as photos must be previously unpublished.) (more photos on inside back cover)

Medication

Adaptation	4
Skimming Credit Card and ACH Payment Details from Tigerpaw Software Clients	8
The Pipe Dream of Sensible School Internet Policy	10
Windows Subsystem for Linux. A n00b5 Toy?	12
TELECOM INFORMER	13
Towards a Secure Telephone Network	15
Ghosting an Operating System for Privacy	17
Tracking Wi-Fi Devices with Python and GPS	18
HACKER PERSPECTIVE	26
Industrial Control Systems and Cybersecurity	29
Bad ISP OpSec	31
Anonymous Temporary Storage and Retrieval	31
How to Become a Hacker in 24 Hours	32
Thinking in AI	33
LETTERS	34
EFFECTING DIGITAL FREEDOM	46
Fun with Text to Speech	47
Hacker Email	49
Cerebral Spill	49
OhNoDaddy: GoDaddy Compromised	50
Book Review: *The History of the Future*	51
ARTIFICIAL INTERRUPTION	52
The Rise of the Machines - Learning to Detect DGAs	54
Responsible Disclosure of a Malware Infiltration Attempt	57
Fiction: Hacking the Naked Princess 0x19	59
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66

Adaptation

The fact that this issue is even here proves how much we are capable of adapting. True, we're more than two months late and it will take some time to recover from that. But for a while, it looked like our future was very much in doubt - or actually, fairly certain of not being there at all.

Let's be clear. Our problems are nothing compared to what so many around the world have been going through since our last issue. The COVID-19 pandemic has shut down our worlds in almost every way imaginable. What we witnessed was like something out of one of those post-apocalyptic movies where all elements of society simply disappear or fall into chaos.

We saw abandoned cities, shut down schools, closed businesses, financial panic, and more fear and uncertainty that most of us have ever seen. Those who lived through war would recognize the taste. Even a traumatic event like 9/11 is but a fraction of what the entire world has been going through. You would have to go back a century to the last great pandemic, where between 50 and 100 million people are thought to have died, in order to realize how truly frightening an event like this is. We're nowhere near that kind of number now (for it to be equivalent - taking population increases into account - the death toll would have to be around four times that), but the signs are troubling and the potential great.

What has happened so far is both shocking and reprehensible. It's shocking because we always forget just how vulnerable we can be, both as individuals and as societies. It can all fall apart so quickly. And at times like these, knowing the difference between what truly matters and what's completely insignificant is what defines the kind of human you are. We've seen a lot of these distinctions lately. There are people who will make tremendous sacrifices in order to help those around them and to ensure that we get through this as best we can. Then there are those who couldn't care less about anyone else. They are the ones who hoard vital supplies and don't lift a finger to help others. And somewhat ironically, their selfishness turns into a sense of imperviousness, and they soon start ignoring safety guidelines and acting as if they're somehow above the virus. Were it not for this attitude, we believe the crisis would be nowhere near as dire as it is today.

This chain of events played out during the 1918-1920 flu pandemic referenced above. A serious outbreak occurred early in 1918 that affected mostly the elderly and sick. But the second wave that followed in the latter half of the year was far more deadly, affecting mostly young adults who were otherwise in good health. Had that first wave been quelled, it's likely the second wave wouldn't have had the same devastating results. While there are many factors that have changed in the past century, not the least of which is our knowledge of medicine and science, there are too many similarities for us to feel comfortable. Those who reject science in favor of politics or religion are given far too much leeway to destroy the lives of innocent people. We stand helplessly by while those at the upper echelons of power continually make the *wrong* decisions and favor greed and their own personal ambitions over what is right and logical for the health and safety of all. When we find ourselves being proven correct when the disease spreads among those who didn't wear masks and observe social distancing, often at the behest of their leaders, we feel no joy. We feel anger. None of this had to happen.

We've seen not only how quickly things can fall apart, but also how quickly people can react when they've finally had enough. It took the murder of George Floyd by police in Minneapolis this May, just the latest in an incalculable string of police killings against members of the African American community, for people in every part of the nation to rise up and demand change. The brutal attacks by even more police on peaceful demonstrators and members of the press did more to shine a light on this sickness than any protester could. When the president himself threatened citizens exercising their right to free speech with the full force of the military, he also proved their point better than a thousand marches. Soon that morphed into the actual seizing of citizens off streets by unidentified federal agents in American cities. While our Constitution and basic military protocol, at least in theory, protect us against such madness, the fact that this is where we are at this point in time is almost as frightening as the pandemic. Put the two of them together and you'll soon realize that the kind of unhinged lunacy that somehow managed to get put in charge is directly responsible for COVID-19 spiraling out of control in this country, unlike most other parts of the world where some semblance of actual leadership exists.

We can only hope that people continue to react on such a scale as we've seen with the Black Lives Matter demonstrations, now defined as the largest protest movement in our country's history. The marches, sit-ins, and confrontations resonated everywhere, even in other parts of the world. And within days, we finally started to see those Confederate statues start coming down, Mississippi's despicable flag was changed, and sports teams began to get rid of racist names that they once swore they would never alter. Basically, having everything from military bases to bridges and schools named after slaveholders suddenly became widely perceived as a Really Bad Idea.

Sure, there were those who claimed this was somehow erasing history, when in actuality it was *calling attention* to those parts of history we're not proud of, kind of like when the Soviets toppled their statues of old leaders for the exact same reason and we all cheered them on. There were those who tried to focus only on negative reactions like rioting or violence, completely ignoring the fact that peaceful protests don't cause these things. Corrupt policies and systemic racism do. And, of course, there were those who insisted that this sort of thing in the middle of a pandemic was grossly irresponsible and would result in increasing the spread tremendously. But that didn't happen, most likely because the vast majority of demonstrators acted in a responsible manner and wore masks. Weeks later, no spike had occurred which provided even more evidence of the effectiveness of these small efforts. Also proving the point were those not following these guidelines who saw cases skyrocket where they went to churches, bars, and political rallies. But instead of looking to themselves, they attack science. They attack the press. They label anyone who's not with them as the enemy, no matter what the facts and evidence prove. And it's time the rest of us stop letting them off so easy. We don't have to let our fellow citizens die because of ignorant leaders. We don't have to continue honoring people whose sins outweigh their virtues. The 1700s were certainly a different time and applying today's values to them can be nonsensical. But that doesn't mean we pretend everything was fine and pure. Evil actions transcend honor. And we can all learn more from real history than from the storybook kind. Besides, there is no shortage of noble people to erect statues and name highways for. Instead of resisting this, we should all be taking pride in *their* accomplishments and building a better nation by doing so.

Yes, there's been way too much in the way of tragedy and avoidable death and suffering. We can't fix that. But we can acknowledge that throughout all of this, something better in us can often emerge. We hope we're seeing the beginnings of that. It will only succeed if we focus on progress, not revenge. After all, for those who truly want to see us fail, progress is the bitterest revenge there is.

As mentioned, we did not expect to make it this far. Our spring issue pretty much went straight to the dumpster in many cases. While we printed the agreed upon amount and paid full price both for the printing and the shipping, stores then refused to take it due to the pandemic, meaning we had the choice of having them thrown out or sent back at our expense and then being forced to pay a penalty for not having removed them

from the originating point. Nearly all issues sent to Canada never made it there. Again, there was no restitution, we were expected to pay full price for delivery and even more, and we wound up pouring a tremendous amount of energy and expense into something that many of our readers never even got to see. Some distributors stopped paying us entirely for previous issues due to their own financial challenges, even though those issues predated all the craziness. And our next issue (this one) had almost nowhere to be sent with so many stores closed and uncertainty as to which would be open at the time we sent issues out.

Again, our challenges are immeasurable next to what so many others have been going through, not even taking health considerations into account. The system sometimes seems designed to have the most vulnerable, the most independent fail with no recourse. Large chains have little trouble telling their landlords they're just going to stop paying rent until all of this is over. Independent and small businesses like ours don't get that option. If we try to exercise it, we'll quickly find ourselves out on the street.

Had the setbacks and expenses been shared from top to bottom, nobody would have systematically suffered more than anyone else. The idea that people are losing their homes because they can't pay expenses after the pandemic cost them their jobs is another indication of our failure as a society, whose first rule should always be to support its members.

We've tried to be as creative and as positive as we can be. We managed to get a number of our spring issues sent to grocery stores instead of dumpsters. We figured since we had so many extra issues that had nowhere to go, why not at least try an experiment and see if we might get something positive out of all of this? We're glad we tried, but now we know that a hacker magazine isn't what people are looking for when they go food shopping. Our sales figures were far worse than we ever could have imagined. So yeah, another setback. But it still felt better than sitting around watching everything fall apart.

And then there was HOPE. We had already been through so much in planning the Hackers On Planet Earth conference for 2020. Just working on doing a better job dealing with disruptive elements that we experienced in 2018 had taken a great deal of effort and attention. Then we lost Hotel Pennsylvania when they opted to triple our price, which would have made it impossible for most of our attendees to participate. But then we found a great new location at St. John's University in Queens which opened up all kinds of options we never had before. It would be a big change, but the hacker community lives for that sort of thing.

Of course, all of those challenges and efforts wound up meaning nothing, as no physical conference of any sort would be possible in the summer of 2020. This became more and more obvious throughout the spring. And, as *2600* is dependent on HOPE for survival, losing the conference on top of all of the other challenges we were dealing with seemed like we were approaching our final chapter.

At least, that's what any reasonable person would conclude.

As we've pointed out so many times in these pages, hackers don't think like most people do. We tend to be creative, thinking outside the box, and willing to do things nobody else has ever tried before. And, faced with oblivion, that's exactly what a bunch of us wound up doing.

The thought was that instead of adding to all of the disappointment of the year and canceling HOPE, why not simply redefine HOPE? While the thought of an all-virtual conference sounded incredibly lame to almost all of us, we sought to figure out ways to make it into something better than just a bunch of webinars and Zoom meetings. For one thing, we realized that if we were going to do this, we had to come up with something bigger than what we were used to. So we started by tripling the amount of time HOPE would last for - from three days to nine days. That started to get people's attention.

But it was about so much more than that. We knew we had some truly incredible speakers. If we could get them enthused about this and have them present what they were going to talk about in a remote environment instead, perhaps that same enthusiasm could still be communicated. Sure, it would be weird not having a visible audience. But, through a combination of prerecorded talks and live question and answer sessions, we could get the best of both worlds.

Then we sought to do something else that was bigger than expected. We decided to get *nine* keynote speakers, one for every day of the conference. Having so many allowed us to reach out to all different parts of the hacker world. And we wound up with a truly incredible variety of fascinating speakers, all with specific relevance to the hacker community, all truly happy to be there. It turned into a real celebration of what we're all about.

We wound up being deluged with talk submissions - more than we had ever received before. That alone helped us erase any doubt we had about the wisdom of going ahead with this event. The energy level was palpable. People seemed to really *need* this after months of losing one thing after another. We had a similar response with workshops, where attendees could participate one-on-one with instructors. We had a few missteps figuring out how to get people signed in to specific classes, but got it figured out and were able to quickly respond to attendee questions and concerns. In the end, we had more workshops than we ever had before and they were well attended and every bit as active as the in-person kind.

We also managed to have villages, like our traditional lockpicking village, as well as everything from hackerspaces in various parts of the world to anarchists to radio broadcasters and enthusiasts. We even managed to have a film festival - not the kind where you go and watch films, but the kind where you go and *make* films during the period of the conference. The fact that people were able to be a part of the conference *and* be able to create full-fledged productions was nothing short of incredible. And then, of course, there were the musical performers, typically getting on stage at around midnight and impressing the global audience with creative and unusual productions. We had never before been able to have this many artists spread over such an extended period of time.

Throughout it all, we used an open standard and lightweight protocol for real-time communication known as Matrix to keep attendees communicating with each other and with speakers and presenters. This worked far better than we had envisioned and brought with it advantages that more mainstream services like Discord didn't offer, such as the ability to register without giving up a phone number. As the old phone company ads once said, it was the next best thing to being there.

But, as always, it was the attendees who set the tone, many of whom were actually able to make it to HOPE for the first time since no travel was required. And in this case, their mood of support, optimism, and eagerness was infectious. For one thing, just the fact that they were willing to support the conference by holding onto their tickets made us realize that there might actually be a future for us after all. We offered refunds to anyone who couldn't do this, but the vast majority opted to stick it out. Were it not for them, none of this would have happened and this very issue would not have eventually made it out. Those particular attendees will always be very special to us and will always get preferential treatment for anything in the future that we're involved with. We in turn pledge to support those individuals, establishments, and organizations that we believe in and that we want to see survive. At the conference, we helped raise nearly $15,000 for the Electronic Frontier Foundation and spread the word about numerous other just causes. Never has the time been more important to show that kind of support.

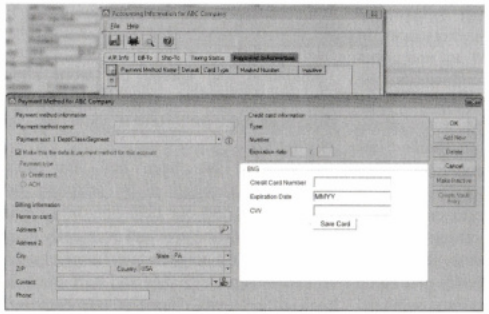
This year has been hell. But we're all getting through it by adapting our expectations and our behavior. In a crisis, that is how you survive and eventually bring things back to a normal state. In society, that is how you create change and start down the road of progress. Through our combined adaptation, the challenges of 2020 will ultimately guide us to a better world.

SKIMMING CREDIT CARD AND ACH PAYMENT DETAILS FROM TIGERPAW SOFTWARE CLIENTS

by Victor

Tigerpaw Software develops and sells business software to run day-to-day operations: everything from sales to service; inventory to invoicing. They'd recently integrated payment processing by credit card or ACH into the stack. Tigerpaw, it must be noted here, is used primarily on Windows PCs. While a web version can be installed and used, this article is focused on the desktop client. This is a story of how I came to discover a flaw in their credit card processing implementation. It was discovered on version 1.17.1.01, which may not have been the latest at that time, so this could affect versions slightly older than that, but definitely not versions 18+.

Bear with me while I cover some background about Tigerpaw and how I became curious about their online payment tools. Tigerpaw's payment processing is handled through a third party company who provides an API to access a "vault" for accepting sensitive financial details and payment processing. The typical vault is designed so that sensitive details are not stored locally. Sensitive details are instead securely passed to the third party company. A token is received back from the third party company which represents the payment method stored in the vault. This token is used to charge the customer in future transactions. The token is worthless to anyone other than the business, so the sensitive financial details belonging to customers can't be stolen in the event of a data breach. This is all good! Using this type of payment vault reduces a company's PCI compliance requirements.



We signed up with this third party company, BNG, who provides the vaulted payment processing through Tigerpaw. To use their service we were required to file a "Self Assessment Questionnaire" (SAQ) to be considered PCI compliant. Alternatively, we could pay an additional $25 a month if we didn't file a SAQ, but, amusingly, we are not absolved from liability or responsibility if we opt to pay the monthly penalty instead of attesting to our level of compliance. I digress, but this agreement was with yet another third party company to BNG, so we're three middlemen deep at this point, which made it difficult to get through to someone who understood (or cared about) our concern.

I believe we were originally presented with SAQ-C, a weighty document covering all kinds of scenarios and policies which made little sense for such a small company. We had processed credit cards through QuickBooks, PayPal, and Stripe which worked similarly for years without any agreement. Among the many questions that didn't seem to apply to us was one asking if all sensitive details were transmitted securely. We sure hoped so, but we weren't the ones who wrote the software, so how could we attest this to be true? At this point, I was given the green light to spend some time investigating!

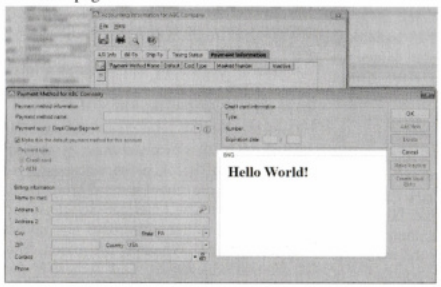
The first thing I decided to do was log all network activity while creating a secure vault entry. I was lazy, so instead of a packet capture I went on the firewall and made a rule to log all network connections emanating from my desktop. I quickly learned that Tigerpaw made web requests during the exchange. There were no fancy services running on dedicated ports, just a few web requests.

I moved onto proxy logs on the firewall to see if I could identify specific web request types and URLs. One interesting entry stands out: an unencrypted GET. Curious to see what was being pulled, I directed a browser to load the URL. It was a form to enter credit card or ACH details! It turns out that Tigerpaw just embedded a web form into its desktop GUI. I took a peek at the source code for this page and the form POSTed sensitive details to an HTTPS url, so at least sensitive details were being encrypted, but I was pretty certain this single unencrypted web request could be abused.

At this point, I decided to spin up a virtual machine and get some tools to thoroughly inspect the process. I installed mitmproxy, arpspoof and some Python frameworks, namely Flask, so I could serve web pages; I configured the attack VM to allow packet forwarding. Then, from the attack VM, I poisoned my desktop's ARP cache with arpspoof, making the VM the man in the middle, so all traffic going through the gateway passed through the VM first. Finally, I configured the VM to intercept and send all unsecured web requests to mitmproxy and I was ready to try serving arbitrary content in place of the payment detail form.

Mitmproxy allows you to write rules to handle specific requests. So, for example, when a request for "tigerpawbng.azurewebsites.net" is received, I can direct that request to my Flask server instead of the real destination. I started a Flask project returning a simple "Hello World" and began creating a new customer payment method on my desktop again.

- Tigerpaw requests the credit card entry form.
- The request goes to my VM, the MITM, instead of the real gateway.
- The VM's mitmproxy sees a request for "tigerpawbng.azurewebsites.net" and directs the request to the Flask server.
- The flask server serves up a "Hello World!" page.



It worked! Tigerpaw showed "Hello World!" instead of the credit card form!

My next task was to grab the source for the real credit card entry form, so I could create an indiscernible fake with one change: modify the URL to which this form submits so it went to my Flask server instead of the real destination. Further success: with a few print() lines added to my Flask project I could now log credit card or banking routing numbers that a user entered into Tigerpaw!

This is pretty bad on its own but, as the project stands, my server only receives sensitive details and leaves the Tigerpaw client in a broken state. I had a few ideas to fix, this but none of them were entirely transparent. I wanted to be the middleman for the whole transaction - capturing sensitive details while not breaking the process. At this point, I have to admit, I spent a whole lot of time that ultimately did not contribute to the final solution. There were some TLS encrypted exchanges in the full process which contained details necessary to handle the entire transaction myself. After quite some time I decided it wasn't possible to accept the sensitive details then go on to complete the transaction, at least not without installing a fake TLS certificate on the client.

I had given up for the day, but the problem occupied my mind through the night. It dawned on me at some point that the Tigerpaw desktop GUI was rendering a web page in an embedded browser and that browser would likely run JavaScript. I wondered if I could:

- Direct the secure POST request to my flask server as before.
- Log the sensitive details as before.
- Reflect the original form back to the client with their payment details filled so the next time it's submitted it will go to the real destination.
- Include some JavaScript to make the client click the submit button after the page loads.

This worked and was completely transparent to the user! I wrote up the pertinent details and got the attention of the company's president and lead developer to report the problem. It has since been fixed. This bug, in my opinion, was most likely a development holdover. The form was available through https, it just wasn't pulling from that URL. It could have also been a misunderstanding that since the details were ultimately POSTed securely that serving an unsecured form wasn't

dangerous.

As for the document BNG and their third party required us to sign, we finally were able to reach someone who understood that we were not directly processing payment details and, since we were using their secure vault, a less stringent agreement, SAQ-A, was sufficient. It could just be a misunderstanding, but I suspect they purposely push the full SAQ to customers to reduce their liability by offloading it onto clients.

While I'd theoretically known how all these components worked for years, this was the first time I combined an array of tricks to discover and craft a real world exploit with criminal potential. I also learned that the small amount of time it takes to look for bugs in obvious places can have a big payoff.

The Pipe Dream of Sensible School Internet Policy

by akerch

The American public school system has always had a strange relationship with students' technological autonomy. When I was growing up in the 2000s, technology in school was viewed with caution and resistance more than anything else: Kid Pix and TypeToLearn were the only applications readily and independently usable by students on school computers, and getting online without a teacher in the room was an uphill battle at best. For better or worse, as I aged, this challenge only excited me and my peers, and the thrill of getting past a district firewall created an urge in me to poke holes in security systems that still motivates me to this day.

Now that I work as an elementary school's IT specialist and can once again stick my fingers into the inner workings of public school district technology and security policy, I feel I must report back some concerning news: while technology, access to the Internet, and availability of hardware have grown and changed dramatically in schools over the years, the district-wide playbook for cybersecurity is almost entirely unchanged. Still, to this day it appears as though district cybersecurity departments spend most of their energy trying to keep students off of individual websites and platforms that they deem dangerous instead of prioritizing the security of the district and network as a whole. In other words, inside the great firewalled garden that is a school district's network, security measures are typically put in place to police the students (and faculty) inside the garden instead of making sure that the garden is safe from outsiders to begin with.

At a recent call I attended with other IT workers from my district, we discussed a multitude of security concerns, but predictably the main one held among many was the rise in popularity of TikTok, and the necessity (according to them) of blocking access to it on the district's network. Aside from the very valid concern of phishing, there was practically no discussion of possible security issues that could arise from sources outside of the school's network. There was no mention of our students' unbelievably easy to guess default account passwords, no mention of the increased reliance on Google for account information and personal data storage, and no mention of the school-specific WordPress sites which are frighteningly out of date (when I started working at my school in 2019, our site had not been updated since 2013). TikTok was truly the main concern.

TikTok is, of course, a place where students can conceivably come across "bad" content, but to spend time and energy attempting to prevent students from getting there in the first place seems not only impossible but also tremendously misguided. District IT departments can obviously block any request going in or out of the network with "tiktok" in the header, but they would be ignorant to think that that would prevent students from accessing the app. Proxies and firewall-circumventing websites are as old as time, and still work darn well. This is not even to mention the glaring hole ripped open in school Wi-Fi networks by cellular data. Even the least tech-savvy student can turn off Wi-Fi in school and use data to open apps and websites a lot worse than TikTok, and they can even create a hotspot to let their friends on, too!

But no, TikTok is a main concern. Funnily enough, YouTube receives none of the caution that is given to TikTok, perhaps because it is more established in the school system? More familiar to teachers? Owned by American Google, innocuous and patriotic, unlike subversive and mysterious Chinese TikTok? Whatever the reason, YouTube is deemed educational, and TikTok is deemed evil, despite the reality that TikTok is at worst a classroom distraction, and YouTube is at worst an incubator for school shooters. But I digress.

To be clear, TikTok is indeed a risky place to be online. Only time will tell what information gets shared and to whom by way of TikTok, but it's hardly more concerning in that sense than any other social media platform. Singling it out as Public Enemy Number One on district networks won't fix that, and doing so will only divert energy away from preparing for the inevitable break-in that will happen to a district that, from the outside, is laughably insecure. And of course, my school district is neither the only district to have vulnerabilities like this, nor the only district to so blatantly ignore them, and frankly, I'm very worried for the day the you-know-what hits the fan, especially if it happens right now during remote learning, when the integrity and accessibility of a school district's network is more important than ever.

Students respond best when they are told the truth, and when they are given independence and responsibility. We would be much better off educating them sincerely about the risks that come with online activity, and allowing them a degree of online autonomy in a space where they don't fear judgment or repercussion for accessing sites that have been deemed non-educational. We can still make sure students are being safe online (I am not arguing for the unblocking of pornography on school networks), while also communicating to them that we trust them and that they are worthy of trust. And to top it all off, we won't have to constantly keep tabs on which new social media sites to block, and can instead spend energy making sure the sensitive data we have access to is kept safe!

Realistically, I understand that this might be a pipe dream, and that large-scale shifts in perception like the one I'm advocating for don't usually happen without an impetus. All I can say is I hope we come out of that impetus in one piece. Until then, I don't have too many problems with pesky school firewalls breeding more hackers.

HOPE
★★★★★★★★★★★★
2020

Not What We Were Planning At All

With a combination of unfortunate circumstances, creative thinking, incredible support, and unbelievable skill and talent, the hacker community made history this year. HOPE 2020 was a magical nine-day event that brought the world 130 talks, 60 workshops, a musical performance each night, and an absolutely amazing community atmosphere. While we all wanted an in-person gathering, HOPE 2020 turned into something truly unique that really brightened a lot of summers (and winters since the southern hemisphere could also participate this year)!

We already have thumb drives ready for those who want quick access to all of the talks in full HD non-DRM MP4 format that will play on pretty much anything and which can be copied and shared as much as you want. Just $79 for two huge drives crammed full of talks plus a bunch of extra stuff. Full details at store.2600.com or write to *2600*, PO Box 752, Middle Island, NY 11953 USA.

If you were a ticket holder or presenter and you haven't heard from us regarding your special shirt and badge, please contact us at hope@hope.net. We can never thank you enough for saving our asses this year and helping to make this incredible event possible. But we intend to try.

Windows Subsystem for Linux. A n00b5 Toy?

by P4!nt

This article should have been written a lot earlier and probably has been. But Microsoft had included a nifty little feature into Windows 10 called the Windows Subsystem for Linux. When I first saw the Windows Subsystem for Linux (or WSL as it's called), I originally thought it was a useless terminal emulator for n00bs to call themselves "hackers." So out of curiosity, I thought "what have I got to lose" and went through the process of installing the required stuff for it and installing Ubuntu (not the 16.04 version that is also on the Microsoft Store).

After it installed, I sat through the 20 minutes it took to install (thanks to my Western Digital 5400RPM hard drive). After I had made an account and password, I was greeted with what I expected: a blank prompt with `user➥name@win-desktop`. It reminded me of the Ubuntu terminal (namely Xterm), and I decided the first thing I was going to install was a nifty program called neofetch. (For those who don't know, neofetch displays system info in the terminal.) So right off the bat, I have to mention, run `sudo apt-get update` *first* or you will run into errors just like I did. So one update and neofetch installed later. I found out that it did indeed work like it should. And one line interested me: `Kernel: 4.4.0-17134-Microsoft`.

So it was indeed a Microsoft bastardized Linux kernel (most likely modified to talk to the NT kernel) running Ubuntu 18.04 just like the kernel should.

I should add that, much like normal Ubuntu, it comes with nano installed which is pretty nifty. And I mention nano to bring up something else: you can indeed run X on this thing. But it's sort of a process to get it running and the only mainly functioning desktop environment is xfce4. But there are some limitations. Namely, you can only really use xfce4 as a desktop environment and even then it somehow takes a performance hit. On my machine, for some reason, audio did not work, but it worked on my laptop. So mileage may vary on audio. And the worst of it all was that sometimes the X server would not work and, when it did, you were mainly stuck with xfce4. I tried i3 and MATE with no real success. i3 kept coming up with errors and MATE just crashed the X server.

But is it a n00b toy? Honestly, no. Yes, it does seem childish, but Microsoft actually introduced something that is useful to Windows 10. Now, yes, it is kind of unfair that I tested Ubuntu when there are a few others on the Microsoft Store (mainly Debian, openSUSE Leap, and Kali Linux). Ubuntu is the one I see a lot of beginners and n00bs going towards. In the end, I see the Windows Subsystem for Linux as a helpful tool to assist people getting into Linux, and for some to get Linux-based tasks done on Windows without the need for dual-booting.

The Rig I tested WSL on:

```
CPU: AMD FX-6300 @4.25Ghz
RAM: 16GB (4 x 4GB) DDR3-1600
HDD: 1TB 5400RPM WD Blue,
320GB Toshiba 5400RPM,
160GB Hitachi 5400RPM
GPU: 2 x Nvidia GeForce
GTX 750Ti OC Edition
OS: Windows 10 Pro
```


TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! When I wrote the spring column, we were the first place in the country to be experiencing the effects of the pandemic. Now the virus is tearing through the country, killing thousands of people every day with no end in sight, and the government seemingly has no plan to get it under control. All of this has had a profound impact on the telecommunications landscape.

While voice services are regulated (and have been carefully and resiliently designed over decades to continue working through periods of extremely high demand), data services are not. The dirty little secret of telecommunications is that capacity is oversold. Just like airlines sell more seats than they have on the airplane (hoping that they "win" and get to keep a nonrefundable fare as pure profit when people fail to show up for their flights), Internet and telecommunications service is also oversold.

There is a really big difference between how airlines oversell and how telecommunications firms oversell, though. Suppose that an airplane has 100 seats and, based on historical data, the airline knows that on a given flight, 20 people on average fail to show up. The airline might, conservatively, decide to sell 110 tickets in order to pocket the difference, and they'll usually get away with it. If 110 people actually do show up, the airline will upgrade a few of them to first class and will offer the rest of them vouchers to take a later flight.

Would you believe that here in the Central Office, we oversell our capacity by *ten times*? For every bank of 400 lines of service coming in from the frame, the switch only has capacity to handle 40 of them at any given time. If you have ever heard a "fast busy" signal or gotten a recording that says "all circuits are busy now, please hang up and try again," you've experienced a grade of service failure (try calling +1-509-457-0051 for a test recording). Oversubscription extends throughout the system; interoffice circuits, tandem circuits, and long distance circuits (+1-541-967-0006) are also oversubscribed. But the only recording you'll be hearing from a coin station without depositing 50 cents is on +1-206-343-0011!

Telecommunications networks are set up with the ability to configure emergency overflow announcements, too. For example, if there is an emergency, long distance carriers may play a related announcement (`www.➥youmail.com/community/greeting/➥earthquake_in_the_area` is an example of one such AT&T announcement). An example "heavy calling" overflow announcement can be heard at +1-313-849-9906 as well.

You might wonder why all of this is the case. Wouldn't it be better to just build capacity for everyone to make calls whenever they want to do so? Well, yes, but it's *really expensive* to build enough capacity for everyone to use the network at once, so this never happens. Instead, we build only what we expect that people will actually use. This is the field of "traffic engineering" and it's a highly structured discipline. Traffic engineers get involved in the initial construction of telephone exchanges, but they also get involved when updates to our infrastructure are needed based on changing calling patterns. For example, we used to have far fewer circuits to mobile phone providers than we do now, and we only had direct interoffice trunks to two wireless providers (both of which we used to own). For the rest, we'd haul everything back to the tandem, causing frequent queuing (it is exactly what it sounds like, and causes your phone calls to take a long time to go through) and outright grade of service failures both at the tandem and on our own switch. Traffic engineers to the rescue!

These days, we work with all regional mobile providers to reliably send and receive traffic directly via VoIP trunks, often bypassing the tandem entirely.

Growth isn't the only story in a regional economy, especially when you're selling traditional land line telephone service. Demand for our services here in the Central Office has considerably changed in the past decade; we are mostly in the Internet business for residential customers these days. Internet subscribers aren't required to bundle telephone service and the company doesn't encourage them to purchase it because it isn't profitable (you can't even buy residential telephone service online). Deployment of fiber to the node has shrunk the footprint of our frame, and our switch has far more capacity than needed for our current subscriber base. While we had been holding reasonably steady with business telephone service, we're processing a tidal wave of disconnections due to pandemic-related business failure. These businesses won't be coming back, and inertia has been one of the only things keeping our traditional landline telephone business operating. While we can't easily consolidate Central Offices, I think we'll likely see investment in smaller, more modern, and more efficient digital switches. Once the company can convince Public Utility Commissions to go along with a full migration to VoIP services, it's likely that we'll primarily service Internet subscriptions from the Central Office, and telephone switching will be consolidated to one or two locations per LATA, as mobile telephone service providers do at their MTSOs.

Traffic engineering is largely a statistical exercise, originally invented by Agner Krarup Erlang, a Danish mathematician. When traffic engineers make their initial "grade of service" calculations, they'll develop a statistical model to determine which traffic patterns they expect to see. This isn't only informed by historical traffic, but what they expect to see in the future. The company employs a full-time economist, and part of this role's duties involves working with traffic engineers to estimate how rapidly a given area's demand for telecommunications services will grow. The math gets pretty hairy, but if you're into that sort of thing, you can learn about the formulas typically used at `en.wikipedia.org/wiki/Erlang_distribution`.

One thing that strikes fear into a traffic engineer's heart is a letter from the state Public Utility Commission. They'll usually learn about this from a very unhappy manager, and the issue will typically involve grade of service failures to e911 services. For the most part, Public Utility Commissions have stopped regulating quality of service, and even service grade. However, service grade to e911 services is strictly monitored and enforced with heavy fines for service failures. Traffic engineers spend a lot of their efforts ensuring that public safety needs are met.

"Quality of service is our problem, and grade of service is their problem" is our mantra here in the Central Office. If calls are failing to go through due to busy circuits, it wasn't our decision to under invest in the network and this doesn't impact our metrics. However, if subscribers are reporting service trouble due to faint volume, scratchy circuits, or the other issues that can bedevil us, it does impact our metrics. While we don't get a lot of trouble reports about telephone service quality these days, Internet is another story entirely.

Remember our friends, the traffic engineers? They didn't plan for the Internet during a pandemic. Residential Internet service has been carefully engineered to carry popular streaming content over periods of peak demand, not for nearly everyone running VPN connections to work at full speed all day and then running video conferences on top of it. Almost overnight, network planning assumptions were out the window. Commercial-grade Internet services are still needed in central business districts, because of all of the VPN connections. But equal capacity was needed for *residential subscribers*, and these networks just weren't provisioned to handle the additional load. Everyone is scrambling right now with traffic profiles that have changed to make pretty much every residential neighborhood look more like busy college dorms full of hyper-connected students than typical boring suburbs. Our trouble queue is full of service complaints. But fortunately, all of this is unregulated! The Public Utility Commission can complain, but they can't fine us.

And with that, I'm going to light up some new fiber. Stay at home, stay safe, wear a mask, wash your hands, and enjoy all of the extra buffering.

TOWARDS A SECURE TELEPHONE NETWORK

by Dave D'Rave

Analog telephone systems were invented in the 1870s. First-generation digital telephone systems (T-1) were developed in the late 1950s. Neither were specified with any thought to the requirements of security or privacy. We are living with the results of those decisions today.

It should be possible to build telephones which are compatible with the current infrastructure, which can do the following:

- Originate and receive calls with high-quality end-to-end encryption.
- Originate calls using secure signals, such that third parties cannot read the metadata.
- Receive calls using authenticated signals, such that Caller ID cannot be spoofed.
- Originate (non-secure) calls to legacy telephones, with or without Caller ID.
- Receive calls from legacy telephones.

Encryption of the Voice Channel

There are a variety of methods which allow secure voice communication, if you have good key management. Modern microprocessors are very powerful, and good quality crypto can be implemented without excessive battery use. You can read about the details of modern crypto and man-in-the-middle attacks on your favorite website.

Let's just say that good crypto exists, but that many exploits exist. One of the best exploits is the plain old fashioned "bug the place in which you are using the phone" method, which defeats all of the other crypto you may be using.

The main idea behind these proposals is that telephone calls should normally operate in an end-to-end encrypted mode, that the two directions should use different encryption keysets, and that the keysets should change for every phone call. Each phone call should generate unique session keys using some kind of hardware random number generator.

The proposed crypto method for voice is to use 14-bit linear encoding sampled at 40k, compressed using some kind of lossy algorithm (wavelets are a good choice), packetized, and then encrypted using one of the Rijndael family of algorithms. This will probably require 100 KBaud of physical bandwidth for high-grade voice quality.

Secure and Authenticated Metadata

To make a phone call to someone without delivering any metadata to the phone system, you will need a telephone session server. Most IP phone systems can support this. The proposed method is as follows:

- You enter the number you wish to call.
- Your local phone then connects to the server and transfers the various information needed over an encrypted command channel.
- The server then calls the person you wish to talk to. If they have a standard phone, then the Caller ID says whatever you want ("Santa Claus 800-NOR-POLE"), or it says nothing. If they have a compatible phone, then the server will deliver an authenticated packet, which contains the Caller ID to be reported to the user.
- Assuming that the person you want has a compatible secure phone and answers the call, the server will authenticate them, transfer the session keys for voice encryption, and you can start talking.

This procedure means that, as far as the phone company is concerned, you made a call to the server, and the server made a call to your friend, but there is no connection between the two of you. Being able to make calls without giving metadata to the switching network is an important first step towards secure and private communications.

Various methods could be used to further obscure the metadata. One idea is to use call-back: When you originate a call, the initial setup procedure results in a very short call, followed by the server calling you back using a different number (typically one with no Caller ID). Another method is to have the server periodically change modes from "cell phone data plan" mode to "digital voice mode," which would appear to the unwanted observer to be an incoming fax or something.

Degrading Traffic Analysis

An important category of hostile data collection is traffic analysis. By observing how many packets go from the person originating the call versus how many packets go from the person receiving the call, some idea can be

gained about the call contents. The solution is to send random packets at random intervals, so as to balance out the apparent data flow.

It also may be a good idea to send dummy traffic on the command channel to obscure, for example, which time zone a phone is operating in.

Key Management and Authenticated Data Transfer

The usual way to attack these kinds of systems is to engage in a "Man in the Middle" attack. The typical way to prevent such attacks is to use public-key cryptography, with authorized servers and their authorized public keys pre-registered. As a practical matter, the server's public key needs to be installed at the factory.

There are several levels of secure communications in the system. First, there is an authenticated/encrypted channel between the originating phone and the server. Second, there is an authenticated/encrypted channel between the server and the receiving phone. Third, there is end-to-end bidirectional encryption between the two phones.

Compatibility with 802.11 and IP Phone Systems

This system of telephony can be used with conventional voice channels, and it can also be used with packet voice or data channels. The physical medium could be anything with sufficient bandwidth/latency, which obviously includes the Internet.

One interesting feature is the ability of this system to run the control packets over a different channel from the actual voice, which enhances metadata security. For example, you could run the voice packets over a cell phone data network, but send the setup, authentication, and management packets over a non-related 802.11 connection.

Compatibility with Non-Secure Phones

While phones which do not support end-to-end encryption will not be as secure, there are still certain advantages to using this system. Metadata will be partly obscured, and incoming calls can be scrubbed against spam much more efficiently if a phone server is handling the routing.

In addition, a smart phone could be programmed to give a red flash or a distinctive ring when a non-secure call is incoming, which would give the operator the option of declining the call based on its security level.

More Advanced Features

Secure conference calls require a server that supports individual encrypted links. It also requires that the conference device itself has access to the unencrypted voice data. Conference calls inherently operate at a reduced level of trust.

A somewhat better secure conference call server would consist of multiple inbound (receive-only) voice channels, along with a standard conference call device which is in a secure location. The effective security of such a system would depend critically on the physical security of the server, and on the use of VPN technology to disguise the physical location from IP scanning.

Tor is probably not a good idea. For one thing, it seems that more than half of the Tor gateways are controlled by national intelligence agencies. For another thing, Tor has poor latency characteristics.

Technical Details of Layer 1

The usual operating mode for this type of device is some kind of packet-oriented low latency network, such as the CDMA technology used by cell phones. Generally speaking, any fast Ethernet-type network will work.

When connecting over an analog network, such as POTS or "Analog Cell Phone," the voice traffic must be converted into digital signals using an analog modem. (This is 1980s technology.) While the connection will work, voice quality may be degraded substantially.

When connecting to a legacy (non-encrypted) phone, voice quality will be limited by whatever the non-encrypted channel supports.

Technical Details of Layer 2 and Layer 3

The usual issues of MAC address spoofing and VPN setup apply. If you are using a VoIP system, it is probably a good idea to identify calls as "fax data" or "compressed video." If you are using generic Internet connections, packets can be identified as "HTTP traffic" or "FTP traffic."

Ghosting an Operating System for Privacy

by Diana

Upon wondering how to return privacy to home and hobbyist computing, I thought of an idea I applied on another system as a patch when track zero of the hard drive was damaged. I feel this idea could aid in providing a ghost portion of an operating system to prevent snooping or spyware or unauthorized data gathering.

The way to think of it is that surgically removing parts of an operating system can take vast amounts of time, especially if you do not have an interrupt map or operating system jump table. The method I'm describing relates to a solution I performed in the 1980s with a Xerox 820 that ran CP/M, and it is still applicable today.

When I received the Xerox 820, I rushed the startup sequence for the 20MB hard drive that came with it. As a result, track 0 was damaged. So, when a program ran and a warm boot was needed, a disk error would appear.

I wanted to fix the disk error because the hard drive contained other programs added when I bought the Xerox 820. I realized my Osborne 1 and Xerox 820 both ran CP/M and, as a new graduate in computer science from University of Wisconsin, my studies included computer science, computer engineering, and operating systems.

So, to fix the program, I studied how CP/M on the Osborne acted when a program ran for a cold boot. The primary mechanism was that rather than have a program end with a HALT statement in assembly, the programs actually ended with call $e000+WarmBoot ; BIOS select for jump table.

Since the WarmBoot constant related to a certain index in the BIOS jump table and the BIOS jump table was loaded into RAM, this meant the table could be modified. So, the code for WarmBoot is 0. When you look at the jump table for $e000, you will see the code "jmp WarmBootMain".

Looking at the "WarmBootMain" code, I thought that maybe I could ghost the original warm boot routine with a ghosted routine that would remap track 0 on the hard drive and use track 0 on the "A:" floppy drive. When I looked at the code, my ghosted OS for "WarmBootMain" was the same except for one line of assembly. The assembly to specify the drive:

```
MVI A, 03h ; set to hard drive
➥C:
Call Bios+SetDrive
```

And was changed to

```
MVI A, 01 ; set to drive A:
Call Bios+SetDrive
```

As a result, when I used the Xerox 820, part of the startup process was to put a special setup CP/M disk in A drive with a submit script to link to the hard drive and add the modified ghost code. This was done by writing a small loader assembly program and then block moving an area open in RAM above the BIOS.

Very reliable and it always worked. When my dad was alive, he would show friends as he was proud about how I worked out a neat hack to get the full system to work.

On current computers, the biggest issues regarding privacy are communications ports and Wi-Fi drivers. As many of us know, when you bought a laptop circa 2005 and reinstalled the OS, you had a special CD that included installing the Wi-Fi driver. If the Wi-Fi CD was not used, even with the Wi-Fi part of chip on the CPU, there was no code to use it, so it was shut off.

In areas where the Wi-Fi driver code is located, if one could devise ghosted code which would feign talking to the Wi-Fi device but, actually send the data to port NULL, then one could control their privacy better than an air-locked computer.

The reason I say one could control their privacy better than an air-locked computer is because an air-locked computer uses a patch that sets a gate as to which data can go to the Wi-Fi part of the chip - which mean it still uses the BIOS software part of the OS. So, a ghosted BIOS would act better because most people would see the same BIOS code when looking at the machine code, not realizing the ghosting.

Tracking Wi-Fi Devices with Python and GPS

by Columbo
Twitter: @columbo2600

It's no secret that in today's society most people are tracked in one way or another. This tracking is often morally ambiguous. One could argue that by tracking your every movement Google is making life more convenient. Google can tell you when there's a lot of traffic on your morning commute. Google would love to give you directions to wherever you want to go. Google knows where you work, and even where you live. Some may argue that this goes a bit too far.

That being said, I'm not writing this for the sole purpose of starting a discussion about morals. I'm writing this to introduce you to a Python script I made for this article called wifitrack. Wifitrack was built to run on Linux. Wifitrack can track and map Wi-Fi devices. I did not design this script with any specific use case in mind. I created it for fun, and to possibly open some people's eyes to methods of tracking that they would have been unfamiliar with otherwise.

You might question if this tracking script I've put together is immoral. I do not believe that the program itself is immoral, but I do encourage you to only use it for good. I think exploring this world of technology is essential for keeping things healthy. Some things may need to change in the future, but we'll never know what to change if we don't experiment.

In the process of making this, my eyes were opened to things that made me feel like some big changes should be made either to the Wi-Fi spectrum itself or in device manufacturers' code. The main thing that comes to mind is that a device's real MAC address (a unique identifier) is thrown all over the place in clear text even when it's connected to an encrypted network. It would be easy to spoof the MAC address every time it connects, but almost no one does this. This set of conditions allows wifitrack to work.

Also, please note I will be using the term "hardware address" a lot instead of "MAC address." An access point's MAC address is also known as a BSSID, so if I'm talking about either type, I will just say "hardware address."

This Python script that I wrote has several options. The first two options are merely for prepping your hardware and the last option returns your Wi-Fi card to normal. The real fun starts with option #3, which uses a GPS device and a Wi-Fi card in monitor mode. It can map out all the devices in a given area. You could in theory make note of how many of a specific manufacturer's TVs are in a certain area and compare that to another area. You could drive by hospitals and get a look at all the equipment (probably including active medical devices) they have connected to Wi-Fi. You could even drive by places with voting machines and see if it looks like any voting machines are connected to Wi-Fi.

Output from wifitrack (option #3 and option #5) is easy to import into satellite mapping programs like Google Earth. Give your output file a .CSV (comma separated value) extension and select the latitude field and the longitude field when importing.

A list of partial hardware addresses and the corresponding manufacturer name can be used to help identify devices. Option #7 of wifitrack will download a manufacturers list taken from Wireshark and make a number of necessary modifications to it so we can use it with the script (make sure you're still connected to the Internet and not in monitor mode). If you'd rather make your own manufacturers list, you can create a CSV file with a row for the known beginning of a hardware address followed by another row with the name you want to use for that manufacturer. You don't need this list, but you will be prompted for it unless you have one with the name "hwvenderlist" in the directory where you run wifitrack. You can just press enter and leave this field empty if you'd rather.

Another important thing to note about option #3 is that it runs an instance of airodump-ng in the background. All of the data will be dumped to a CSV file and the file name will be the date and time you ran option #3. This file or files, depending on how many times you run this option, will give us some basic information about whatever devices are around. Option #6 will sift through all of the data airodump-ng dumps and give us device probes from a specific MAC address that you specify. It will also say which access point this MAC address was associated with if any. This brings me to my next point.

Our devices are often very noisy. If you have the Wi-Fi enabled on your phone, even if you're not at home, there's a chance your device will try to probe your home network. Why is this a big deal? Well, there's a large wardriving database out there known as `wigle.net`. You can search `wigle.net` for an access point's ESSID or BSSID (your access point's MAC address). If your device is asking for your home network and you have a unique access point name, someone could look that up and find out where you live. (The same can be said if you take a screenshot of all of your available access points and share it online. Don't do that unless you don't mind being geo-located.) The probes your device makes can also just tell a story about the places you've visited and the Wi-Fi you've connected to.

If you're trying to find a target from only one location, you might want to try using a blacklist file. A blacklist file will let you ignore all the addresses on the blacklist. Run option #3 in the location when your target and presumably your target's device are not in the location. You can use the output from the time your target wasn't around as a blacklist file for when your target is known to be in the location. This will work better in a location with very little activity. You will be prompted for a blacklist file every time you run option #3, but you can leave the field blank if you don't want to use one.

The blacklist file could also be used to continue your progress on option #3 if you have to restart wifitrack for any reason. Just use the name of the output file you want to continue using as the blacklist file, and then again as the new output file name. Wifitrack will just append the new data and you won't get any repeats of devices you already detected.

Option #4 of wifitrack may give you yet another reason to turn your Wi-Fi off in public places. To clarify, I don't just mean you shouldn't connect to open Wi-Fi. I mean if you don't want to be tracked, you should probably just disable Wi-Fi completely in public (not to mention Bluetooth or just your phone in general). You could mitigate this to some degree by spoofing your MAC address every time you connect to an access point, but depending on which device you use, that could be more or less difficult.

Here's a bit of a thought experiment. Let's say you wanted to find out the MAC address of Donald Trump's unsecured Android phone to force him to look at lolcatz. Let's pretend that he carries this phone around the country to all sorts of public speaking events. Let's also say that, hypothetically, the people surrounding him at these events change from day to day. If you want to follow the president around, you can run option #3 of wifitrack every time you are in close proximity of the president. Option #4 will let you compare multiple option #3 outputs and find any hardware address matches from file to file. If Trump keeps his Wi-Fi on, you could find his phone's MAC address by process of elimination. Now that you have his phone's MAC address, you could work some wizardry to make him look at cute cats... but perhaps that's a topic for another article.

The last feature we have to talk about is option #5. This option requires that you enter at least one hardware address in a text file that you want to watch for. You can add multiple addresses and you can label them by adding a comma immediately after the address followed by your label (example: "ff:ff:ff:ff:ff:ff,label").

You will also be given the option to run a command when you successfully come in range of the device(s). I suggest something like "sudo -u username mpv beep.wav&" to play a beep sound from whichever user you'd like. Some audio players don't play well with root, which is what this program was designed for. So in that example, you can select whichever non-root user you want to run a sound effect to alert you.

To test option #5, I made a file that contained the hardware address of my smart TV and turned the TV on. I then drove about a mile away, turned option #5 on, and drove past my place of residence at 35 mph. With no fancy antennas and only using the network card in the cheapest Netbook I could find, wifitrack successfully picked up some packets and took note of the longitude and latitude. Looking at the GPS coordinates on Google Earth, I noticed by coincidence or not that the plot point was directly across from the location of the TV.

I also discovered in testing that option #5 could be an excellent alarm to alert you to someone using a specific device. If you ban your child from the TV, you could use the TV's address and set a loud sound to play when it turns on.

In closing, maybe we should all be more careful about what we connect to the Internet. All of these devices can be spied on. Does it matter if a passerby can tell if I'm toasting bread with my smart toaster? I'm not sure, but it sure feels wrong hooking a toaster up to the Internet.

Dependencies

When I tested this on the latest full live Kali build, I only needed to install "gpsd" and a Python module known as "gps". When I tested this on a live Ubuntu build, it was much more complicated.

If you're using Ubuntu (live or not), you might need to edit a gpsd configuration file located at /etc/default/gpsd. If you're using a live version of Ubuntu, you will likely also need to edit or create the /etc/apt/sources.list file to specify the correct repositories. I would recommend you just use Kali.

The following commands should pull in any packages you could be missing (requires an Internet connection):

```
# apt update
# apt install aircrack-ng python
➥ python-scapy iw python-pip
➥ tcpdump gpsd wget sed
# pip install gps
```

Important Links

- *Kali Linux* - www.kali.org - Very nice Linux distro with a ton of pentesting tools.
- *aircrack-ng* - www.aircrack-ng.org - An amazing suite of tools for monitoring Wi-Fi networks or cracking Wi-Fi passwords.
- *figlet* - www.figlet.org - A program that lets you write words in ASCII art font.
- *Great place to get started with scapy* - hack➥oftheday.securitytube.net/➥2013/03/wi-fi-sniffer-in-10-➥lines-of-python.html
- *Kismet* - www.kismetwireless.net - Great program for wardriving. Compatible with Bluetooth and even SDR. This program was definitely part of my inspiration.
- *macchanger* - www.gnu.org/soft➥ware/macchanger - An easy way to spoof your MAC address. Avoid being tracked!
- *scapy* - scapy.net - A Python library for reading and crafting packets.
- *wigle* - wigle.net - A giant wardriving database. There's a good chance your access point is logged in here already.
- *Wireshark* - www.wireshark.org - A great tool for sniffing traffic. As I've explained, I used their manufacturers file to help identify devices.
- My twitter: twitter.com/columbo➥2600 - I will be posting a digital version of the code from this Twitter account shortly after publication. If you have any questions or comments, you can reach me there.

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

#For best results, run as root in a safe enviornment.
#This is experimental software.  Use at your own risk.
#This requires the scapy python library, the aircrack-ng suite, gpsd, and
➥ the gps python library.
#Read the original article for further documentation.
```



```
from scapy.all import *
import os, sys, time, datetime
from gps import *
#Insert some threading to run multiple functions at the same time.
from threading import Thread
#Some variables to use globally later.
menu = ""
interface = ""
hwaddress = ""
#Optional vender list to view the names of the hardware venders.
venderlist = []
#Our output file's name.
file_name = ""
#Lattitude/Longitude global variables.
lat = 0.0
lon = 0.0
#Menu display.  Title font uses a figlet font named Bloody.  Requires utf
➥ coding.
def displaymenu():
    global menu
    menu = raw_input("\n\
To continue, type a number and then press enter:\n\
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
➥ *\n\
Choose an option:\n\
1. Change into monitor mode with airmon-ng.\n\
2. Start gpsd and specify your gps device.\n\
3. Scan for all hardware addresses and write to file. ctrl-z to exit.\n\
4. Match hardware addresses from different file outputs.\n\
5. Scan for one or more specific hardware addresses from a file.\n\
6. Find probes and associated devices from a hw address.  This scans through
➥ your airodump-ng database.\n\
7. Create or update hardware vender file to identify most devices scanned.\n\
8. Stop monitor mode and return wifi to normal. \n\
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
➥ *\n\
")


#----------------------definitions-----------------------
def AddressScan(pkt) :
    global file_name
    global lat
    global lon
    splitstring = []
    f = open(file_name, "a")
    venderfound = 0
    thetimeis = datetime.datetime.now()
    #This section looks for valid harddware addresses.  The length will be
➥ 17.  Then it looks through your hardware vender file
    #to figure out which type of device the address belongs to.  It also takes
➥ note of the date/time and gps coordinates.
    if pkt.addr1 not in clients and len(str(pkt.addr1)) == 17:
        clients.append(pkt.addr1)
        for line in venderlist:
            if len(line) > 2 and line[2] == ":":
                splitstring = line.split('	')
                if str(pkt.addr1)[:len(splitstring[0])] == splitstring[0].
➥lower() and venderfound == 0:
                    f.write(str(pkt.addr1) + "," + splitstring[1].rstrip()
➥ + "," + str(lat) + "," + str(lon) + "," + str(thetimeis) + "\n")
                    print "Device Found: %s - %s,%s,%s,%s" % ((pkt.addr1),
➥ splitstring[1].rstrip(), str(lat), str(lon),str(thetimeis))
                    venderfound = 1
        if venderfound == 1:
            venderfound = 0
        else:
            f.write(str(pkt.addr1) + ",unknown," + str(lat) + "," + str(lon)
➥ + "," + str(thetimeis) + "\n")
            print "Device Found: %s,unknown,%s,%s,%s" % ((pkt.addr1),
➥ str(lat), str(lon), str(thetimeis))

    if pkt.addr2 not in clients and len(str(pkt.addr2)) == 17:
        clients.append(pkt.addr2)
        for line in venderlist:
```

```
            if len(line) > 2 and line[2] == ":":
                splitstring = line.split(',')
                if str(pkt.addr2)[:len(splitstring[0])] == splitstring[0]
➥.lower() and venderfound == 0:
                    f.write(str(pkt.addr2) + "," + splitstring[1].rstrip()
➥ + "," + str(lat) + "," + str(lon) + "," + str(thetimeis) + "\n")
                    print "Device Found: %s - %s,%s,%s,%s" % ((pkt.addr2),
➥ splitstring[1].rstrip(), str(lat), str(lon), str(thetimeis))
                    venderfound = 1
        if venderfound == 1:
            venderfound = 0
        else:
            f.write(str(pkt.addr2) + ",unknown," + str(lat) + "," + str(lon)
➥ + "," + str(thetimeis) + "\n")
            print "Device Found: %s,unknown,%s,%s,%s" % ((pkt.addr2),
➥ str(lat), str(lon), str(thetimeis))

    if pkt.addr3 not in clients and len(str(pkt.addr3)) == 17:
        clients.append(pkt.addr3)
        for line in venderlist:
            if len(line) > 2 and line[2] == ":":
                splitstring = line.split(',')
                if str(pkt.addr3)[:len(splitstring[0])] == splitstring[0]
➥.lower() and venderfound == 0:
                    f.write(str(pkt.addr3) + "," + splitstring[1].rstrip
➥() + "," + str(lat) + "," + str(lon) + "," + str(thetimeis) + "\n")
                    print "Device Found: %s - %s,%s,%s,%s" % ((pkt.addr3),
➥ splitstring[1].rstrip(), str(lat), str(lon), str(thetimeis))
                    venderfound = 1
        if venderfound == 1:
            venderfound = 0
        else:
            f.write(str(pkt.addr3) + ",unknown," + str(lat) + "," + str(lon)
➥ + "," + str(thetimeis) + "\n")
            print "Device Found: %s,unknown,%s,%s,%s" % ((pkt.addr3),
➥ str(lat), str(lon), str(thetimeis))

def scancommand(pkt) :
    global file_name
    global hwaddressfile
    global lat
    global lon
    global systemcommand
    f = open(file_name, "a")
    if pkt.addr1 in clients:
        thetimeis = datetime.datetime.now()
        print "Device Detected: %s, %s, %s, %s, %s" % ((pkt.addr1), clients
➥[pkt.addr1], str(lat), str(lon), str(thetimeis))
        f.write(str(pkt.addr1) + "," + clients[pkt.addr1] + "," + str(lat) +
➥ "," + str(lon) + "," + str(thetimeis) + "\n")
        if systemcommand != "":
            os.system(systemcommand)
    if pkt.addr2 in clients:
        thetimeis = datetime.datetime.now()
        print "Device Detected: %s, %s, %s, %s, %s" % ((pkt.addr2),
➥ clients[pkt.addr2], str(lat), str(lon), str(thetimeis))
        f.write(str(pkt.addr2) + "," + clients[pkt.addr2] + "," + str(lat)
➥ + "," + str(lon) + "," + str(thetimeis) + "\n")
        if systemcommand != "":
            os.system(systemcommand)

    if pkt.addr3 in clients:
        thetimeis = datetime.datetime.now()
        print "Device Detected: %s, %s, %s, %s, %s" % ((pkt.addr3), clients
➥[pkt.addr3], str(lat), str(lon), str(thetimeis))
        f.write(str(pkt.addr3) + "," + clients[pkt.addr3] + "," + str(lat) +
➥ "," + str(lon) + "," + str(thetimeis) + "\n")
        if systemcommand != "":
            os.system(systemcommand)
    f.close()

def channelhop():
    channel = 1
    while channel < 14:
        os.system("iw dev %s set channel %d" % (interface, channel))
        time.sleep(.01)
```



```
        channel = channel + 1

        if channel == 13:
            channel = 1

#This feature requires you to set up gpsd on your system.  Also requires the
➥ python module gps.
def gpsfunct():
    global lat
    global lon
    gpsd = gps(mode=WATCH_ENABLE|WATCH_NEWSTYLE)
    while True:
        report = gpsd.next()
        if report['class'] == 'TPV':
            lat = getattr(report,'lat',0.0)
            lon = getattr(report,'lon',0.0)

def airodumpdatabase():
        #Run airodump and save all the data. we can refer to this data later.
➥ This line uses the -K 1 option to run airodump-ng in the
        #background.  If this option isn't used airodump-ng seems to override
➥ the output.  This will keep on running even after the
        #python script is closed.  You may want to close it manually when
➥ you're finished.
        os.system('airodump-ng -K 1 -w' + "aird-db/" + str(datetime.datetime
➥.now()).replace(" ","") + ' --output-format csv ' + interface)
#--------------------menu-----------------------------
while True:
    displaymenu()
    if menu == "1":
        os.system("clear")
        #Assumes the user has iwconfig.  Shows available interfaces.
        os.system("iwconfig")
        #User inputs preferred wireless interface
        interface = raw_input("Please enter your wireless interface:
➥ (ex. wlan0)\n")
        #Device is turned off and then put into monitor mode
        os.system("ip link set dev " + interface + " down")
        os.system("airmon-ng start " + interface)
        #If you type in your interface name incorrectly you should restart.
➥ The other options will assume you succesfully entered monitor mode.
        interface = interface + "mon"
    if menu == "2":
        gpsdevice = raw_input("Please enter your gps device.
➥ (ex. /dev/ttyUSB0)\n")
        os.system("gpsd " + gpsdevice + " -F /var/run/gpsd.sock")
    if menu == "3":
        #Start GPS function so that can load while prompts are entered.
        Thread(target = gpsfunct).start()
        clients = []
        clients.append("ff:ff:ff:ff:ff:ff")
        #User inputs interface if string is empty.
        if interface == "":
            os.system("clear")
            os.system("iwconfig")
            interface = raw_input("Please enter your wireless interface:
➥ (ex. wlan0mon)\n")
        if os.path.exists("hwvenderlist"):
            venderfile = "hwvenderlist"
        else:
            venderfile = raw_input("Please enter the name of the file with
➥ hardware venders, or leave this blank.\n")
        if venderfile != "":
            vf = open(venderfile,"r")
            for line in vf:
                venderlist.append(line)
            vf.close()
        blacklistfile = raw_input("Enter the name of your blacklist file or
➥ leave this blank and press enter.\n")
        if blacklistfile != "":
            bl = open(blacklistfile,"r")
            for line in bl:
                #Truncate the line to 17 characters.
                clients.append(line[:17])
            bl.close()
        file_name = raw_input("Please name the output file.\n")
```

```
        if file_name == "":
            file_name = "wt-option3-default-output-" + str(datetime.datetime.
➥now())
        #Checks for airodump-database directory.  Creates it if it doesn't
➥ exist.  We can use these files later.
        if os.path.exists("aird-db") == False:
            os.system("mkdir aird-db")

        #Press ctrl c OR ctrl Z to stop scripts
        #Runs our channel hopper, address scanner, and airodump-ng database.
        Thread(target = airodumpdatabase).start()
        Thread(target = channelhop).start()
        Thread(target = sniff(iface=interface, prn = AddressScan)).start()
    if menu == "4":
        list1 = []
        list2 = []
        file1 = raw_input("Enter the name of your first output file.\n")
        file2 = raw_input("Enter the name of your second output file.\n")
        savedfile = raw_input("If you would like to save the matches to a file
➥ enter a file name.\n")
        f1 = open(file1,"r")
        f2 = open(file2,"r")
        #Check to see if the user wants to save a file.  Otherwise you'll get
➥ an error.
        if savedfile != "":
            nf = open(savedfile,"a")
        for line in f1:
            list1.append(line.lower()[:17])
        f1.close()
        for line in f2:
            list2.append(line.lower()[:17])
        f2.close()
        for line in set(list1).intersection(list2):
            print line
            if savedfile != "":
                nf.write(line)
        raw_input("Press enter to return to menu.")
        os.system("clear")
    if menu == "5":
        Thread(target = gpsfunct).start()
        if interface == "":
            os.system("clear")
            os.system("iwconfig")
            interface = raw_input("Please enter your wireless interface:
➥ (ex. wlan0mon)\n")
        clients = {}
        hwaddressfile = raw_input("Please enter the filename that contains the
➥ addresses you would like to scan for\n")
        file_name = raw_input("Enter the name of the file to output successful
➥ scan info.  (date/time GPS)\n")
        if file_name == "":
            file_name = "wt-option5-default-output-" + str(datetime.datetime.
➥now())
        systemcommand = raw_input("Enter a shell command to run on a
➥ successful scan. (ex. vlc ring.wav)\n")
        hwf = open(hwaddressfile,"r")
        splitstring = []
        for line in hwf:
            splitstring = line.split(",")
            if len(splitstring) > 1:
                clients.update({splitstring[0][:17].lower() : splitstring[1]
➥.rstrip()})
            else:
                clients.update({splitstring[0][:17].lower() : "no name"})
        Thread(target = channelhop).start()
        Thread(target = sniff(iface=interface, prn = scancommand)).start()
        hwf.close()
    if menu == "6":
        splitstring = []
        airdfile = []
        airddb = os.listdir("aird-db")
        clientmac = raw_input("Please enter the mac address of the
➥ client.\n")
        clientmac = clientmac.upper()
        for line in airddb:
            ad = open("aird-db/" + line,"r")
```



```
            #We start scanning from the bottom.  The first line we need is len
➥(airdfile)-2.
            linenum = 2
            for line in ad:
                airdfile.append(line)
            #Checks for a colon on the 3rd character of the line.  If it's
➥ there it should be a client.
            while airdfile[len(airdfile)-linenum][2] == ":":
                splitstring = airdfile[len(airdfile)-linenum].split(',')
                #Prints out the associated client.
                if splitstring[0] == clientmac:
                    print "Associated AP:"
                    print splitstring[5]
                if splitstring[0] == clientmac and len(splitstring[6]) != 2:
                    for probe in range(len(splitstring) - 6):
                        print "Probe:"
                        print splitstring[6 + probe]
                linenum = linenum + 1
            ad.close()
        raw_input("Press enter to return to menu.")
        os.system("clear")

    if menu == "7":
        #We start out with the wireshark manuf file.  That has all the info
➥ we need.  It just has to be modified.
        os.system("wget -O hwvenderlist-tempfile-delete https://raw.githubuser
➥content.com/wireshark/wireshark/master/manuf")
        #Get rid of all the commas.  We need to turn this into a csv file
➥ of sorts.
        os.system("sed -i 's/,//g' hwvenderlist-tempfile-delete")
        #Replace the first tab on each line with a comma.  This should
➥ separate all the hardware addresses.
        os.system("sed -i 's/\\t/,/' hwvenderlist-tempfile-delete")
        #Truncate the "netmasks" after the specified number of bits.
        os.system("sed -i 's/0:00\\/36//' hwvenderlist-tempfile-delete")
        os.system("sed -i 's/0:00:00\\/28//' hwvenderlist-tempfile-delete")
        splitstring = []
        ieeereg = ""
        #We need to move all the IeeeRegi addresses to the bottom.  Some are
➥ redundant after modifying the netmasks.
        with open("hwvenderlist-tempfile-delete", "r") as fdownload:
            with open("hwvenderlist", "w") as output:
                output.write("# This file has been modified for use with
➥ wifitrack.  Sorry for any confusion.\n")
                for line in fdownload:
                    splitstring = line.split(",")
                    if len(splitstring) > 1 and splitstring[1][:8] ==
➥ "IeeeRegi":
                        ieeereg = ieeereg + line
                    else:
                        output.write(line)
                output.write(ieeereg)
        fdownload.close()
        output.close()
        os.system("rm hwvenderlist-tempfile-delete")

    if menu == "8":
        #User inputs preferred wireless interface.
        if interface == "":
            os.system("iwconfig")
            interface = raw_input("Please enter your wireless interface:
➥ (ex. wlan0mon)\n")
        #Device is turned off and then put into monitor mode.
        os.system("airmon-ng stop " + interface)
```

The Hacker Perspective

by Dave Collins

Not unlike asking 100 anarchists "how do you define anarchism?" if you were to ask 100 hackers how they would define a hacker, you might get just as many answers. I am a longtime anarchist, but someone who would only recently and reluctantly called themselves a hacker. So keep in mind that this is just one dude's (skid's) opinion about what a hacker is. If you disagree, that is fine. If you think that the definition of a hacker should be more nuanced, that is also fine. You should write your own article next time! For this essay, I propose the following definition.

A hacker is anyone who figures out solutions to problems using the tools available to them.

Ideally, the solutions to these problems would be elegant, but sometimes a quick and dirty hack that works is worth as much as a perfectly polished exploit. I am not going to get into a semantic discussion about "crackers versus hackers" - for the purposes of this column, the color hat worn by the hacker is entirely irrelevant. I don't even think it is necessary to limit this definition to computers. In the end, when one finds a solution to a problem, or gets the desired result, the question of "how" is not that important. Sure, it can be tremendously interesting, but does it *really* matter why something works or *that* it works? Put another way, do you need to know how a particular exploit works against a particularly vulnerable system, or simply that it does?

Rather than have a restrictive definition of a hacker that involves compromising vulnerable computer systems, I would rather have a larger definition of a hacker to encourage more people to start thinking critically. Life is too short to try and act as arbitrator of a term, policing people's language about how they choose to define themselves. Our world has too many bullies in it, and anyone who would bully someone about how they define themselves is an asshole I don't care about. If your first reaction to someone calling themselves a hacker is to sneer and try to prove that they aren't, you need to take a long, hard look at yourself. I will return to the gatekeeping issue later because I think it is really important.

I became a hacker because of a series of happenstances. Let's start with professionally. After being burned out working as a network administrator for my hometown community college, I moved across the state - first to earn a BA and then a graduate degree in a subject (history) that gives me basically two options: either go earn a Ph.D or teach at a high school. Since I didn't get accepted to any of the doctoral programs I applied to after finishing my MA, and I was unable to find any academic work, a friend (who would later turn out to be my first mentor) told me about the basics of vulnerability scanning and explained how to set up a small consultancy. Fortunately, I started using Linux before going to college and have been using it daily for nearly a decade. So when it came time to start using Kali Linux for a touch of the ultraviolence, I knew how to get around the command line. I spent a few months teaching myself the basics in a really poorly constructed lab environment and asking my mentor a ton of questions. I even found a client that let me poke around their website. After that, a company nearby offered me a junior consultant position and I took it. Next thing I knew, I was getting paid to try to hack into banks and other businesses - a dream come true for the kid who grew up watching the movie *Hackers* and thinking that there could be no cooler job then getting paid to hack all day.

So when I mentioned earlier that a hacker is anyone who figures out solutions to problems using the tools available to them, let me give you a practical example. I was at a client's site (in this case, a bank) and we were doing a little physical recon as we were leaving the building. In hindsight, we should have done this when we first came in, but that is not the point of the story. The point is that I discovered two potential vulnerable spots in the client's network based on weaknesses I knew about because of my time first at the help desk and later as a network administrator. So when I say that gatekeeping is a problem, this is part of what I am talking about. Just because I didn't know how to really write code at the time, or develop my own exploits, I could have still leveraged previous IT knowledge to compromise the network in a way that someone who only has development experience wouldn't know.

So even though I'm not in the best position to offer a message to aspiring hackers, I'm going to do it anyway. First of all, you have to be willing to fail. Often. When I popped my first shell on a client, it was using an exploit that failed four times before finally working. Information security as a field is one where you are simply going to fail. One dirty secret that professional penetration testers and red-team people hate to admit is that blue teams are good. They are often really damn good. Just because you are able to pop a shell, that doesn't mean it will stay alive. Or that your connection will stay alive. If you want to be good, you have to first be willing to admit that you suck. Perhaps worse still is the knowledge that you are going to suck for a long time. Let me give another example.

I started the PWK course offered by Offensive Security, you know, "Penetration Testing with Kali Linux?" Anyway, going into it, I didn't have a ton of programming experience. I'd taken a few classes at the aforementioned community college, one or two on UNIX programming at another school, and have been teaching myself Python for the last few months, but I am not a great coder yet. I still have a ton to learn. Going through the course, you are expected to be able to write scripts and do the basics of exploit development. While these things are both fun, they also require you to fail, a lot. Anyone who has written code can tell you that your code is going to fail. You will figure out new and unique ways to make it crash and burn, but baby, it is going to burn. I've written code that borked machines so badly it crashed both the virtual machine and the host that was running it.

To paraphrase Jake from *Adventure Time*, sucking at something is the first step to getting good at something. In infosec, as in life, you have to crawl before you can walk.

So in addition to the message above, get used to sucking. The next bit of advice I would give to the aspiring hacker is to find a mentor: someone who knows more than you, and can point you in the right direction when you get stuck. Setting up a decent practice lab can be a pain in the ass. Having a mentor who can help walk you through it and give you nudges when you get stuck is worth its weight in gold.

Third bit of advice: Google is your friend. Perhaps, secretly, more than a friend. Sure, you have to cough up some of your personal data, but really, it's the price you pay for the best search engine. You can find all sorts of cool stuff by using the right magic words.

Fourth bit of advice: get ready to fail more.

If you are willing to fail, be rejected, do some Googling, and you are fortunate enough to find someone to point you in the right direction, you still have a mountain of work to do. Even though hackers can sometimes have reputations for being lazy, the reality is that many awesome hacks are awesome because they save you from having to do more work.

Near the beginning of this article, I had mentioned that I would talk about a few reasons why I thought that gatekeeping is bad. I want to expand on this further, because I think it is worth talking about. Information security, as a professional field - if you believe the hype and what you would read online - is desperate for people. Warm bodies who can do anything from working in a SOC (Security Operations Center - monitoring alerts, tweaking firewalls, and overall trying to ensure that the networks they are watching over remain secure and uncompromised) to penetration testing, exploit development, reverse engineering, threat hunting, malware analysis, bug bounty hunting, and even more - the information security subsection of the information technology field appears to be growing and shows no signs of slowing.

What this means is that, like it or not, there are going to be more people coming into the field. Some people take the hard line with newbs and skids and won't want them to feel welcome. Hazing and trials-by-fire still exist as well, but I don't think that this is the best way forward. If we all want to get better, having more people to bounce ideas off of is the best possible outcome. Most free and open-source software advocates are aware of the many eyes theory, but if you aren't, the idea is that many eyes make shallow bugs. Put another way, the more people that can look at code, the more likely we all are to find vulnerabilities that can then be patched. Or, the more people in information security, the better we can all get, regardless of the color of your hat.

Good news everyone! Systems will remain unpatched! There will always be some "business need" for old software, super old

hardware and operating systems, and stuff that just should not ever touch the Internet to be totally touching the Internet! Sysadmins and netadmins will insist that for "reasons" they can't patch their stuff, at least not immediately, because ya gotta test patches! So, while they test patches, their vulnerable shit is just sitting on the Internet one quick Shodan search away! Plus, with the expansion of the Internet of Things (IoT) even *more* stupid shit will soon be touching the Internet, and IoT has a bad reputation for considering security as an afterthought, if they even think of it at all. That means that there will be more microwaves and smart light bulbs to pwn going forward!

What I'm trying to say is, there will be work in information security for a while to come, at least until machine learning and AI puts us all out of jobs (and hopefully just that and not, you know, killing us). Hopefully by then, the need to do 40 hours of work per week will be eliminated, and we can spend more time doing cool shit rather than spending a third of our day at work.

Until that day comes, try to be nice to newbs, skids, and scrubs. Remember that everyone started somewhere. Most people didn't begin writing exploits their first day, or even their first week. While I am sure that there are some who did, most had to rely on the work of others to learn. If you are in a position where you are more experienced, perhaps consider mentoring someone who is new. If you would rather not interact with a person, you could think about writing blog posts or doing video tutorials, which might end up leading to someone reaching out to you. There are also professional reasons why doing such things can be good for your career, if you want to reach the next level. Or, if you just want more Twitter followers, that can be a good avenue as well.

Remember, if you want to be a hacker, you can totally do it. It won't be easy, you will fail over and over again, but you will learn - almost certainly more then you ever expected you would. Not only about computers, systems, and networks, but also about people. Remember that some will shit talk along the way. There will be nay-sayers, haters, and you might make an enemy or two regardless of the color of hat you decide to wear. Until we can overthrow the capitalist system, we must have jobs. Being a hacker can either be an awesome job by itself, or be a framework you use to help make your life easier. Either way, if you figure out solutions to problems using the tools available to you, then you too can be a hacker. Bonus points if other people consider you a hacker too, but who cares what other people think?

Life is short. Far too short to spend it wishing you could do something. If you have always thought to yourself, "I want to be a hacker!" you can start, today! If you have a computer that is fast enough and with enough memory, find a guide and set up your own lab. Download a few vulnerable virtual machine images, segment them off, and start hacking! It really is that easy. If you don't have a capable machine, you can find walkthroughs that explain how to break the virtual machine images. Start reading walkthroughs for machines labeled easy and read, read, read! Once you get good enough, hack yourself an account on hackthebox.eu. If you are willing to work, you too can be a hacker. Remember that there will always be people who talk shit. If you develop all the skills of a hacker, and your reputation precedes you, the only people crazy enough to talk shit about you will do so behind your back and, like the tree falling in the forest, if you can't hear it, does their shit talk make a sound?

Dave Collins is an offensive security professional who blogs at whateversauce.com and tweets @ whatever_sauce. The author would like to send love greetz to his wife @punkrawkboss.

HACKER PERSPECTIVE
submissions have closed again.

We will be opening them again in the future so write your submission now and have it ready to send!

Industrial Control Systems and Cybersecurity

by Craig Reeds

Let's start with some definitions, to make sure we are all on the same page. An Industrial Control System (ICS) or Supervisory Control and Data Acquisition (SCADA) system is an industrial computer system that monitors and controls a process. This can be everything from flood control pumps, the electric utilities power generation and distribution system, to building cars and making candy bars. Another set of terms I will be using are IT and OT. IT is your normal office Information Technology, where OT is Operational Technology, the sort of technology used in manufacturing or industrial environments.

Industrial Control Systems have been around in one form or another since we started manufacturing things centuries ago. In their current incarnation, they are electronic, computerized systems. With the advent of the Internet and, more recently, the Industrial Internet of Things or IIot, Industrial Control Systems are being pushed into being connected to the Internet. This is a step that can only cause problems.

Connecting Industrial Control Systems to the corporate network and/or the Internet has opened the floodgates to serious cybersecurity risks, threatening to cause billions of dollars in damage and possible death to people and livestock. Even though we are faced with this danger, cybersecurity spending by critical infrastructure companies and manufacturing companies is lagging.

The first computer virus was created in 1981 and up until Stuxnet in 2010, viruses were confined to just damaging computers and could not affect the physical world. Now we are faced with viruses and hacking attacks that are intent on disrupting the physical world. Over the past years, we have allowed Internet-borne cyberthreats to find their way into Industrial Control Systems and cause lots of problems and dangers for the people that work with and around them. A well placed cyberattack can cause human casualties, billions in infrastructure damage, and even bring certain operations of our critical infrastructure to a screeching halt. Cyberattacks such as LockerGoga, WannaCry, NotPetya, Triton, Sauron, CrashOverride, and many of their mutations have proved that Industrial Control Systems are not only vulnerable, but very attractive targets. Some statistics, according to the latest threat landscape for Industrial Automation Systems in H2 2018 data from security vendor Kaspersky:

- Nearly 41 percent of all ICS endpoints were attacked.
- Trojan malware was found on 27 percent of ICS endpoints.
- 26 percent of attacks come from the Internet.
- A survey commissioned by Tenable found that in industries using industrial control systems (ICS) and operational technology (OT), 90 percent of respondents say their environment has been damaged by at least one cyberattack over the past two years, with 62 percent experiencing two or more attacks.
- 37 percent report at least one significant disruption caused by malware and 23 percent report at least one nation-state attack. 23 percent report at least one instance of economic espionage and 21 percent reported an instance of cyber extortion, such as a ransomware attack.

So, now that I have scared you a little, let's look at why these things are happening and what we can do to protect Industrial Control Systems.

Many companies are pushing to combine their IT and OT departments, something they call IT/OT Convergence, and it is really not a very good idea, since IT and OT have differing goals.

IT's primary goals are confidentiality, integrity, and availability - the CIA triad. While doing this, they also try to make it possible for the users to access the network from any location that they are working from, using whatever computing device they have with them. The goal is to make it as easy to work from an airport, hotel room, or coffee shop as it is to work in the office itself. Technology is updated and replaced often. Service packs are loaded, new software releases are loaded, and bugs are fixed.

OT's primary goals are availability, integrity, and confidentiality, a complete reversal of

the CIA triad. They strive to keep production running, be it an electric utility, an oil rig, or a pop-tart factory 24/7/365. In the case of an electric utility, in order to meet the required standards, it is a closed system without the open access provided by IT systems. However, back in January, the *Wall Street Journal* published an article detailing how some bad actors (they said Russians) hacked into the electric grid here in the United States. They were able to do this due to a lack of security on the jump servers at low impact facilities. This vulnerability has been closed, or should have been closed, based on the changes for low impact entities detailed in *NERC CIP-003-6 Attachment 1* which went into enforcement September 1st, 2018 and *NERC CIP-003-7* that goes into effect January 1st, 2020. Something else to realize about this hack is that it started on the IT side of the house. If IT and OT at the attacked facilities had understood each other better, it could have been stopped.

The primary goal of Operational Technology cybersecurity personnel is to make the control systems as secure as possible, and this means controlling how users connect and what they use to connect with. This is accomplished by having very strict firewall rules and only opening secure ports or running services if they can be justified. OT systems such as these were never meant to be connected to the Internet and never should be if the goal is to protect them.

When it comes to OT, it doesn't matter what industry you run a cyber vulnerability or penetration test scan on. You will always find some out of date system, like a Windows XP computer, or a PLC that is pivotal to the operation that has an unpatched security flaw. Many times, systems are running the same software they were when they were installed, patches have not been loaded either because they were never tested by the vendor who supplied the equipment or thought to be unneeded since the equipment isn't connected to the Internet. Remember, some of the OT equipment is 10 to 20 years old; it was never meant to be connected to the Internet. These devices often do not have built in security capabilities because no one ever figured they would be connected to the Internet.

Moving away from the traditional "air-gapped" (no external connections) Industrial Control System to a corporate network or Internet connected system is dangerous. The security procedures, protocols, and protections that make sense for corporate IT cannot be applied to systems that were never created to be connected to the outside world.

When it comes to cybersecurity of Industrial Control Systems, the biggest issue is the lack of Operational Technology (OT) knowledge among cybersecurity professionals. Most everyone has the IT knowledge, but it cannot always be applied to an OT situation. For instance, when running an Nmap or OpenVas scan on an Industrial Control Network, do you know what equipment could lock up if you do too deep of a scan? There is a major difference between IT and OT, and it needs to be understood before any sort of scans are run.

Many universities and colleges have amazing cybersecurity programs that teach the students how to protect and configure all the latest and greatest equipment. Those students graduate ready to stop the evil Bad Actors from attacking corporate networks all around the world. This is a great thing - we need them there, fighting the good fight and providing us with those protections. However, when it comes to Industrial Control Systems like those at our utilities and manufacturing plants, there is a lack of cybersecurity knowledge and support.

So how do we solve these problems?

1. You have potential OT cybersecurity gurus in your maintenance department. Take someone that knows the process and teach them cybersecurity.
2. Resist merging IT and OT into one department.
3. Forget traditional antivirus software and implement application whitelisting.
4. Ensure proper configuration/patch management.
5. Reduce your attack surface area - disconnect from the office network and the Internet.
6. Build a defendable environment - segment the network.
7. Manage authentication - multi-factor authentication.
8. Implement secure remote access.
9. Monitor and respond.

Bad ISP OpSec

by JavinZ (zuckonit)

A lot of popular ISPs (Comcast, AT&T, Verizon) plus countless others have fantastic security - but a noticeable flaw is the default password for customers. You can easily see what these passwords are by finding them on the ISPs' websites or by scavenging forums online to find them. Do ISPs care about this? No. They are just there to make money from the customer.

I will mostly look at Canadian ISPs because they are very close to me. Two noticeable ISPs are Access and SaskTel. One quick look on their websites allows you to find what their default passwords are, allowing you to brute force accounts with a notorious program named "Hashcat." You can easily find out what provider people have from their access point name. A lot of ISPs do this, like Access (example: Access254).

The default password for Access is a random 21-character-length alphanumeric string. If you have a good GPU and CPU, you can crack the password in no time. But for basic users, it would take quite a while.

A worse example is SaskTel, whose default password still can be easily found on their website. SaskTel is unique in that they have the default password as their home phone number. Yes, that's right, their default is the *home phone number*. Now, if you know the area code for your province or region, you can easily brute force it in no time with Hashcat. For me, it took 48 seconds to brute force a SaskTel AP and have access to the devices on the network and, to make it worse, they left the admin panel with the same password as their AP!

If someone is inexperienced in computer security and hacking, and isn't aware of the consequences of leaving stuff with the default password, a lot of bad things can happen to their network without them knowing.

It's always good to change the password on your AP to something strong so nothing like this can happen. Will your ISP help you if you were hacked? Sure! But they won't learn from their simple mistakes.

Anonymous Temporary Storage and Retrieval

by Buanzo

Hello hackers all over the world!

I am not sure if this technique is well known. As far as I can tell, no one is using it (probably for a reason), but I have not seen it covered, so here it goes.

People tend to use sites such as pastebin and other websites to post information to. Some time ago, I was wondering about different methods for saving data to "the Internet" without having to register, validate I'm not a bot, etc., etc. So my mind wandered a bit... "what gets written all over the Internet, directly or indirectly?" *Log files*.

So a simple google dork for access_log and "index of" provided me with a nice bunch of servers publishing httpd access_log. And yes, I could create an interesting URL... for instance:

```
www.example.com/THIS_DOES_NOT_
➥EXIST_YYYYMMDDHHMMSS_ARBITRARY_
➥DATA…
```

and yes, I would find a matching 404 for

```
"/THIS_DOES_NOT_EXIST_
➥YYYYMMDDHHMMSS_ARBITRARY_DATA" in
www.example.com/logs/access_log…
```

Add some Tor there... and presto, you have a way to store data. Add some crypto, some structure... and there you go, a way to store information for a long time (google cache, wayback, etc., etc.) without having to do anything but a simple HTTP GET.

I might put some tools up on GitHub, but please go ahead and have fun with this extremely simple method.

Cheers!

How to Become a Hacker in 24 Hours

by XCM

I must have been 17 years old. In the space of a few weeks, I had developed a morbid obsession with cryptography.

I had spent some time devouring a couple of books I had found on the topic; which was quite an esoteric one at the time in my town.

At the first opportunity, I would stop by the local bookshop to avidly rummage on the shelves in the meager IT section. Having been in the exact same shop just a few days earlier was not a reason to deter me from trying my luck.

As I grabbed a copy of a book that caught my attention, the very same book I had quickly scanned earlier that week, I heard a voice behind me.

"I want a book that teaches how to become a hacker."

I don't know how resolute that statement was. However, fast forward twenty-something years, I still remember that moment as if it was yesterday.

It is not uncommon nowadays to sense a similar level of excitement in those who decide they want to become hackers.

Perhaps more precisely, today many enthusiasts are still fascinated by their very personal ideas of what a hacker is. An idea that has maybe shifted considerably over the last half century.

The challenge, in my opinion, is that at times it is easy to assume there is a clear, proctored path to follow to become a hacker.

Like reading a book.

I personally believe that, depending on each individual interpretation of what makes someone a hacker, the answer on how to become one might or might not be found in a book.

In 2020, literature on the subject is surely much vaster and at least in part of great quality, compared to the days of my misadventures in the local bookstore.

Cybersecurity is now at the forefront of prime time news and it is ubiquitous. Apparently the world will soon implode as all the professionals working in cyber will ultimately retire and nobody else seems to be bothered with embarking in this obscure profession.

For the reasons above, a great deal of attention has been directed at training the new generation of hackers and cyber pros.

This is great news. However, as I sensed in that bookstore 20 years earlier, I have mainly observed the usual recurring approach: focus on tools and techniques and forget about understanding the technologies or human weaknesses that the tools are meant to exploit.

Memorize the OWASP list of vulnerabilities and know which scripts to use to exploit them. Don't worry about understanding HTTP, PHP, SQL, or Linux.

More broadly, just focus on attacking computer networks with such tools rather than, say, opening up the old robot vacuum cleaner and repurposing the multiple motors found inside.

To put it bluntly, the format and approach of most books on security only add fuel to the fallacy of the fast lane to becoming a hacker.

Whereas I agree that learning to use scripts and other software to poke at a host can surely be a captivating starting point, it is a methodology which will sooner or later disappoint in its shallowness.

Moreover, if not assisted by the necessary background research, intuition, and creativity, this can generate a false and dangerous sense of proficiency.

Would you get operated on by a surgeon who knows the tools but does not have much understanding of human anatomy and medicine?

We must convince the new generation of security pros and hackers to focus on building, over time, the necessary understanding of technology and human psychology. Also, more emphasis should be placed on developing critical thinking, problem solving, and people skills.

If my child ever shows interest in what I do for a living, I will try and point out that if they work towards developing the right talent and understanding, they might eventually achieve what it takes to be a successful hacker, chef, doctor, or whoever they will want to be.

In the meantime, I would tell them to just keep questioning and tinkering. Be aware that your choices along the way might make this a very long journey.

Nevertheless, it can be amazing, exhilarating, and extremely rewarding.

Thinking in AI

by Duran

Artificial intelligence... the problem is how to acquire intelligence? It's not a simple thing. Nowadays, we're using computers to simulate human intelligence, making the software or hardware so it can represent human behavior to a certain extent. But it's not enough; it's just starting.

In the next few decades, we may be able to make a major breakthrough in the field of AI. The key step will be to use logic circuits to simulate brain plasticity. Because in the whole process of human life, the brain will continue to generate new neurons and new connections. It will be a very difficult task to simulate this process through the circuit. Apart from this, what's the difference between artificial intelligence simulated by circuit and real human intelligence? Data and algorithms alone are not enough.

For example, how is an AI to understand a person's irony? I criticize a thing with a praise tone. Can machines recognize the inner meaning?

For example, in the story of "Empty City Strategy" as stated by the Chinese historical masterpiece *Romance of the Three Kingdoms*, would machines recognize Zhuge Liang's scheme, or would they think like Sima Yi?

For example, if Lili let Ben ask Mike for a portrait photo for her, would machines recognize Lili has a crush on Mike?

In a word, it's not a simple thing that can be done by programming, deep learning, using lots of if/else statements or switch... case statements. It's a deep level thinking thing that exists in the real human brain. This is something which cannot be simulated by circuit.

Is there any way to solve this? The answer is yes.

In the future, the ultimate form of artificial intelligence will be the combination of artificial brain and computer. Connect the artificial brain to the biosensor and then output the results through the computer. In this way, a certain kind of real AI can be realized.

It's not science fiction. In 2013, through the work of Dr. Madeline Lancaster, she and her colleagues grew the first human-derived "cerebral organoid." In addition, the researcher Alysson Muotri found something interesting in his lab at UCSD and published in *Cell Stem Cell* (29 August 2019) a study that looks in more detail at cerebral organoid electrical activity. It can be predicted that humans will build a cell growth brain finally, but this is a sensitive matter which brings up issues of ethics. Also, there are many people working intensely on hardware. The former Facebook "Building 8" team and Neuralink project from Elon Musk all tried to work out brain computer interfaces.

So, at last, with the development of computer science, medicine, and biology, the artificial brain will be responsible for simulating real brain activity. The brain computer interface (BCI) is responsible for transmitting signals to the computer, and the computer is responsible for calculating the output results. But I have to say, the ultimate AI can't replace human intelligence; it can only be infinitely close to human wisdom.

Although it is not easy, with the development of human society, all problems will be solved reasonably.

CURES

Trouble

Dear *2600:*

Hi, I am reaching out as a long shot hoping to get a reply. Short story... I have an ex who is a hacker, who while we were together did the P**** route and just keep stealing my passwords (they were written in a book, cause I was being hacked so much I had to keep changing them and couldn't keep track) so he gave my fb, my gmail, my Samsung Cloud (which I had no idea I had), and my Microsoft OneDrive (again I had no idea) and he was uploading *everything*: texts, pics, vids, and of course some not so good. So he gave all these passwords out to his little bitch friends. Some were sending messages in my Facebook to family members telling them I was going to kill myself. He sent emails to my boss that cost me my job, and ultimately the sick fuck did try to get me to blow my brains out. Pfft as if.... I know it's whacked but it's true. He is, however, a skilled hacker and he has my mac address to my router. I have already bought a new computer but I have found pics in this one that I didn't put in it, bookmarks that I never bookmarked, etc... so I am ultra paranoid. I am studying network engineering and going into cybersecurity, I am learning Kali and Metasploit, John the Ripper, Brutus, etc., so I am learning and very fast. But I have googled so many variations of "can a hacker hack my computer if he knows my router's MAC address." No answers.

I just don't want to keep living in paranoia. For real. I mean, I got an *anonymous fax* on my printer when I first relocated (moved out of state) that had no message. My fucking printer isn't set up as a fax and I don't have a telephone line. I assumed he sent it by the IP address of my printer.

So I want to make my shit completely secure. I bought a new router, I plan on buying a new computer in a couple weeks, I need a new one to run virtualization to set up another OS in Hyper-V so I can practice Kali n shit, but I want to be positive this sick fuck can't get into my new shit. Like, should I get a new printer too?

Please don't laugh too hard. Yes, I am a total script kiddie, but hell, I am working on it. Thanks.

Amy

Wow. There's quite a lot here. And, yes, it is tempting to laugh. But we don't have to.

The main point to convey here is that people gain more power with the perception of what they might do, rather than what they actually are capable of doing. You're assuming this jerk (yes, we're on your side since you wrote us a letter) is behind every bad thing that happens with any of your devices. You think he sent you a blank anonymous fax, which seems like a pretty strange way to try and intimidate someone. In reality, most likely something was misconfigured that enabled this to happen. You'll find examples of this sort of thing every single day. But if he thinks for a second that you believe he's capable of doing all of these things, then all he has to do is sit back and wait for something to go wrong - because it always does - and he'll get all the credit.

We're not minimizing the bad shit he's done to you, and for that his ass should be nailed to the wall. But what makes you define this idiot (we're getting angrier the more we think about him) as a hacker in the first place? Because he found your book of passwords and started to use some of them? That's not hacking by a very long stretch. He gained access by finding your book (bad idea, never store passwords like that again), entering the passwords he saw, and then pretending to be you. He gets credit for knowing how to read and that's about it.

Having someone's MAC address is not a big advantage. However, if your router is using the same password as it was when you last let this shithead near it, well, that's a problem. Changing the password or getting a completely different router will make that potential point of entry disappear. Then do the same on every other bit of machinery you own. It's really not hard, but it takes discipline. And then you need to be careful with how much info you give out online. If privacy is valuable to you, then you need to protect it. Lastly, stop thinking about this person and his stupid friends, which shouldn't be hard if you moved out of state. They are nothing. Good luck to you and may Mr. Dipshit get back exactly what he has given out with no way of escaping it.

Dear *2600:*

Sir please help me that I forgot my Facebook password, on the other hand my mobile number and email are lost due to my mobile theft. Now there is a lot of document on how I can get back my ID.

SSAT

Humans should come with a reset button. Here's a newsflash: you don't lose either your mobile number or your email address if your phone is stolen. So if the scenario was as you say it was, you could get your Facebook password reset by replacing your phone and/or logging in to your email account from somewhere else. But seriously, forgetting your Facebook password could be a real blessing without much of a disguise.

Questions

Dear *2600:*

I've been a subscriber for a few years now, and I love *2600*. Occasionally I'll remember an article and want to read it again, but don't remember which issue it was in. Is there a way to search old archives by keyword or something? That would be really helpful.

Thomas

The newer issues are available in searchable PDF format which makes that possible. The older ones are mostly scans for now. We need for the OCR technology to get a little better so we can get our whole library searchable. Until then, you can at least scan the titles of our articles on our store.

Dear *2600:*

With New York State declaring an emergency and banning gatherings of large numbers of people, compounded with European countries closing their borders, how is it this conference is still taking place?

What preventative measures is *2600* taking to insure that this virus is not spread even further?

A Nonymous

Thanks for asking us this back in early March while everyone was still trying to figure out what was going on and the conference was four months away. Sometimes, admitting you don't know the solution is the right answer. We didn't and nobody else did either. But what we did know was that we weren't going to do anything to put anyone in harm's way. With a lot of imagination, talent, and support from the community, HOPE 2020 evolved into something completely different.

Dear *2600:*

I hope this message finds you well. I am a 22-year-old student from the United Kingdom, and next year I will finish my MSc in computer science. I often visit New England in the summer months and have to say I've fallen in love with its American charm.

Anyway, I have two long-term goals: working in cybersecurity and living in Connecticut. I have been doing some rather exhaustive research on both career paths and immigration and was wondering if you knew of any schemes that sponsor skilled immigrant visas for budding network analysts, security testers, and the like who have Masters-level qualifications? I would be so grateful if you had any details that you might be able to pass on.

Thank you so much for your time. I wish you the best during this unusual period we're living in!

Beckett

We just have to ask. Connecticut? Living in that state is fully half of your long-term goals? We have nothing against it, but why someone from overseas would target that one state is definitely worthy of note. We hope you make it. Unfortunately, our country is not exactly the most welcoming towards immigrants at the moment. Like the recording says, please try again later.

Dear *2600:*

Hopefully this is the right place to email. So I already have a number of issues from you guys, dated back to 2011. I was thinking about getting the full set plus back issues. I don't really need duplicates, but was wondering if I told you what issues I already have, would you be able to just send the unique ones instead of duplicates? If that's not possible, I could just donate the duplicates to the library.

Colin B

We can certainly do that without much fuss if that's what you want. We prefer to always give something back when people invest in us, so maybe we can figure something out.

Dear *2600:*

I used to pick up *2600* at Borders (in the 90s). I was wondering if you still have a physical publication that I could subscribe to, or if you have gone fully digital.

B

In fact, we do! You're likely reading the digital copy, we suspect. We have a thing for paper and we probably will never be able to break the habit. But yes, you can certainly subscribe. What we're curious about is where you found our address that didn't also tell you how to subscribe. Somebody isn't doing their job.

Information

Dear *2600:*

I've been noticing that the Sweetwater County jail in Wyoming has been taking in a significant number of ICE holds recently and I just came across your information. I'll post a couple links and if you want me to find more or whatever would be most helpful to verify this, let me know.

Chris

This is for our concentrationcamps.us project, which sought to identify all of the facilities where potential immigrants were being detained. It quickly got to the point where we just couldn't keep up. This is something we may need to outsource.

Dear *2600:*

Hey Tovarish,

I found your email from the concentrationcamps.us project. I want to take on something similar. After the arrest of Officer Chauvin, it looks like cops can be held criminally liable when there is intense public scrutiny. I'd like to start doxxing cops and building a public database of active police officers. Ideally, the next time someone dies in police custody "accidentally on purpose" like Floyd, police administration won't be able to hide anyone's actions.

Would this be the kind of thing you would be willing to host if I get some useful extracts? Also, learnings or advice from your research above

would be greatly appreciated. Had some success with compiling public documents, but it's a slow process for often outdated information.

Thanks in advance!

Mike

We don't support releasing data on individuals who haven't done anything wrong. We do support revealing names of those who are complicit in crimes with the backing of police or government. That information simply cannot be kept solely by the very organizations that are under suspicion. It's sickening how many atrocities are gotten away with simply due to the job the perpetrator had or their connections with the powers that be. Accountability is a concept many of us seem to have lost all memory of. We all must be treated equally, both as individuals in our day-to-day lives and as suspects when accused of a crime. If data is not forthcoming or if it's being buried, then it's up to the rest of us to liberate it. The trick is doing this in a responsible manner. None of this would be necessary if the system were set up with checks and balances to prevent these abuses.

Dear *2600:*

Did you know that every tire is equipped with a factory-installed GPS chip so that you can be located in 5G networks? If you don't like this, you have to cut off the little antenna sticking out of the rim.

Michel

We did hear about this. It's the bright idea of a company called Pirelli. It can supposedly transmit information about the road surface to you as well as other cars around you. So if you start to swerve, other cars can be alerted to this, assuming the driver somehow doesn't pick up on it. It can also keep track of the amount of miles you drive. And get this. Theoretically at least, your car could hit a pothole and then alert the authorities that they need to fix it and give them the exact location. Your tire could take your place as an angry letter writer to city hall. And while the company is focusing primarily on the safety elements, you can bet there will be a darker side to this technology. We'll be happy to experiment and write about it when these things hit the market.

Dear *2600:*

I am a JFK assassination researcher, and I am very interested in information on Jack Valenti. I am aware of the *2600* lawsuit that happened with JV, and I was hoping I might be able to speak with someone who is knowledgeable about JV, the lawsuit, and any other piece of info on him no matter how small. Let me put it this way; Jack was not in the motorcade as he stated, and I know where he was. His real name is not Jack Valenti. Any information you might be able to assist with would be appreciated. Thank you.

Also, where did the name 2600 come from? It happens to be the Air Force One code for when the plane is in flight and the President is not on board....

C

Well, that's not where we got our name, but thanks for that fascinating tidbit. It's nice to know if the President ever gets kicked off his own plane that our name will be invoked. As for the late JV (we actually got to call him J), he certainly didn't let on that he was carrying some important facts about the JFK assassination. But then, why would he have shared that with the people he was suing? It being nearly 60 years since all that happened, if you know something about his involvement, you might as well let the rest of the world know. Oliver Stone isn't getting any younger.

Dear *2600:*

Four days after leak publisher DDoSecrets circulated private documents from more than 200 law enforcement agencies across the United States, Twitter has permanently suspended its account and falsely claimed that the site may infect users with malware. DDoSecrets describes itself as a "transparency collective, aimed at enabling the free transmission of data in the public interest." Recently, it published BlueLeaks, a 269-gigabyte trove of documents that *KrebsOnSecurity* reported was obtained through the hack of a web development company that hosted documents on behalf of police departments. A Twitter spokesperson confirmed that the company had permanently suspended the DDoSecrets account for violating the social media site's rules barring hacked materials. The spokesperson said the material (1) contained unredacted information that could put people at risk of real-world harm and (2) ran afoul of a policy that forbids the distribution of material that is obtained through technical breaches and hacks, as publishers of DDoSecrets claimed had been done. DDoSecrets co-founder Emma Best criticized the suspension and noted that the Twitter account for WikiLeaks remains active despite its publishing of vast troves of private information resulting from the 2016 hack of the Democratic National Committee and members of the Hillary Clinton campaign. WikiLeaks has also tweeted links to its Vault 7 series, which published details about closely guarded CIA hacking programs. Other accounts associated with the Anonymous hacking movement have also escaped suspensions. Twitter was also slow to suspend Guccifer 2.0 and the Dark Overlord, the monikers of two purported hackers, both of whom also published extensive amounts of personal information obtained through hacking and tweeted the links. "@DDoSecrets has worked with dozens of major news outlets across the world and published terabytes of data uncovering money laundering schemes, corruption, and more," Best tweeted. "Now we're being censored for publishing the #BlueLeaks files about law enforcement.

Chuck

It becomes clearer with every passing day that Twitter is in way over their heads. And it's our own fault for ever taking them so seriously. Inconsistently applied policies coupled with a God complex never ends well.

Feedback

Dear *2600:*

I just finished issue 36:4 and I must say I absolutely loved the article "Reflections on Hackers." This article is part of the reason why I still subscribe to your magazine after more than ten years! Technical articles are one thing which I love reading, but then there are non-technical "hacker culture" articles like this one that really hit home. *Hackers* is also my favorite movie, and growing up I wished constantly I had a close knit group of friends like the ones referenced in the article and movie. Back then, I'd take just one friend that I could talk to computers with that wasn't just obsessed about games. While I did enjoy myself with several hours of *Starcraft* and *Red Alert*, I was the only one of my friends that seemed to realize computers could do so much more than just be used for playing games. I nurtured my passion for computers throughout my adult life, and here I am 20 years later an information security professional.

Keep up the good work!

Sardonyx

It's always great to get a letter like this that appreciates the way we do things. Mixing the technical with the philosophical or the non-technical is part of the magic that makes up the hacker culture. Variety is the key. Thanks for writing.

Dear *2600:*

I enjoyed the article about using Pi-Hole (37:1) to hide yourself from Facebook. Here's another method I think has more advantages. Firefox has a feature called containers. These are like separate user accounts in that they do not share cookies. For example, I can have a "personal" container and a "work" container; the personal container can be logged into my personal Gmail account and the work container in my work Gmail account.

Where it becomes powerful is when you install an add-on called Temporary Containers. This can be configured so that every time you open a new tab or navigate across domains, it throws away the old container and creates a new one. This means nothing can track you via cookies. Combine with a user agent randomizer add-on and fingerprinting is probably impossible. Here's how to configure it.

First go to the General tab and enable automatic mode. Then head to the Isolation tab. Under the Global subtab, expand Navigation and select "different from tab domain and subdomain." Now every time you browse from one domain to another, it will switch containers and, to all the trackers, it will appear as two unrelated users.

This will break sites with SSO logins spanning different domains or subdomains since they can't see each other's auth cookies. For example, I use Google Drive. Their SSO login takes me through accounts.youtube.com and accounts.google.com. In order to be able to login to Drive, I went to the Per Domain subtab and added a new entry using this regex: */(accounts\.youtube\.com\|accounts\.google\.com\|drive\.google\.com)/*

then configured "Always open in" to enabled and "Navigation -> Target Domain" to never. This treats all those domains as one domain to keep in the same container.

A site like Amazon has multiple subdomains. That breaks due to the "different from tab domain and subdomain" configuration above: going from one subdomain to another loses my session cookie. You can loosen that to say "different from tab domain." Or you can whitelist them in the Per Domain subtab like *.amazon.com, setting "always open in" to enabled.

This container approach has advantages over DNS blocking. It confounds *all* trackers, not just the ones I blacklist. It also spams trackers like Facebook with junk data. When I navigate across ten sites today and again tomorrow, they see 20 separate users, useless data that is a liability for them to store rather than an asset.

I can selectively use services that require a login without enabling tracking on their "free" services. For example, with the above Google regex, I can login to use Google Drive and enjoy free Google News in another tab, but the News tab will appear to Google as a non-logged in anonymous user.

Lastly, it helps with paywall news sites that give you a few free articles. Since you always appear to be a new user, you always qualify for a free article! I also use it to navigate glassdoor.com. They require you sign up for an account after one or two page clicks. Using the Per Domain override, I changed the navigation to "always" and now every page click on that site looks like a new user and I have access to all their content without giving them any of my information.

Cloud-hosted Pi-Hole DNS blocking has the advantage of working for all your devices anywhere you take them. It also prevents leaking your IP, which is a problem with Temporary Containers. If there are specific companies you absolutely don't want even seeing your IP address, then combine Temporary Containers with Pi-Hole to blacklist those companies, or use Tor.

David

Thanks for that fantastically helpful and inspiring tutorial. This kind of thing can really cheer people up who feel the battle for privacy is lost. It never will be with this kind of spirit.

Dear *2600:*

Keep up the great work. Your digest is watched for every quarter and read from cover to cover. My wife recognizes the envelope and refers to it as geek porn. I read these more than I ever did a

porn magazine and can truly say I read it for the stories, not the pictures. But I do like the front and the back covers.

George

This is one of the better comparisons we've gotten in a while.

Dear *2600:*

I always get your mag at the local bookstore and just recently started listening to your podcast. Something that caught my attention while listening to your podcast on April 8th, 2020 regarding the coronavirus.

Let me just state I am in no way a political person. I do not vote and all that.

I will say listening to your podcast since this coronavirus has started is pure cringe, starting from April 8th, you continued with 30 plus minutes of you going off about Trump and politics.

I find it ironic that a magazine that has always been about free thinking and not believing government agendas has the host saying the government should do more, and that a government such as China has handled the coronavirus in a better way (going by the numbers we are told), clearly missing the fact that doctors in China were told not to discuss the virus for weeks out of fear.

I do not think we need more government intervention, as this is going to be what happened after the attack of 9/11 when they took more of our rights as American citizens and used the fear as the way to do it. This will happen again with this coronavirus. It just seems that the magazine has gone backwards from its original stance.

I mean the host of the podcast repeated numerous times that the leaders in charge need to mandate stay at home orders. I laugh and say to myself why is it I need a government official to tell me to stay home, when clearly I can read a newspaper and watch the news and see that it's not a good idea to go out using pure logic. I didn't need a government or anyone to tell me to stay home. So using the excuse that the leaders in charge didn't mandate orders to stay home is basically an oxymoron from what you have been standing for the past years.

I definitely can sense a bias with a magazine that honestly should really have no political stand with parties of any sort.

Either way, always a supporter from the early 2000s.

Hope to hear back on the view and stance of this.

2600Submit

Well, there's a lot to cover here. Let's start by saying that you don't have to be a "political person" to vote. And to not vote, especially in times like these, is a pretty defeatist move. Don't you want some say, however tiny, in who gets to make the decisions and the policies? Not voting just enables those who do to make your decisions for you. Realizing that is just common sense, not politics.

Now, as for the government role in all of this, we don't know what you think government is for, but many see it as the entity that holds the responsibility of keeping its citizens safe. And when we see that trust being violated or ignored, you're damn right some of us are going to call them on it. We're thrilled that you have enough common sense not to expose yourself or others to this horrible virus. But, as you can plainly see in the time since you wrote this letter, not everyone possesses this common sense. And those who don't have a really toxic effect on many others - literally. Which is why at press time we're seeing a second spike in infections in precisely the areas where the precautions weren't enacted or taken seriously by the government. For this to happen so late in the game, after so much had been learned through earlier mistakes and later successes, is tantamount to criminal behavior. And Trump is first in line on that charge. By not taking the science seriously, putting his own needs ahead of the people, and doing everything to thwart the efforts of those trying to keep people safe, he can easily be credited with the preventable deaths of tens of thousands of our citizens, possibly more before this is over. So yeah, you're going to hear some direct criticism of someone like that with absolutely no apologies. And that's not a political stance; it's a human one.

Nobody escapes blame entirely here. We can find missteps and bad decisions everywhere we look, in every locality and in every country. But there are some who have acted with wanton disregard for the needs of the people. We don't intend to let any government get a free pass on that count.

Now please go vote. And thanks for the support.

Dear *2600:*

I enjoyed reading ~Me's article about USPS Informed Delivery in 37:1 and would like to add a bit to it. ~Me's premise that enrolling one's address precludes others from doing the same may be incorrect. Until recently, I had two homes in different states, each with its own Informed Delivery account with unrelated login credentials. I sold one home and placed a change of address forwarding order using the account for that address. I was offered, and accepted, Informed Delivery for the new address, which is my other home that already has its own Informed Delivery account. I now receive two emails each day to different email addresses with Informed Delivery info. You can also set up a second address within a single account!

To the postal service's credit, the Informed Delivery service would not start until I entered a code online that I received at the "new" address in an actual letter from USPS. I don't remember if that was the case when I set up the accounts a few years ago.

As to being able to read through the envelope, I can confirm that this happens quite often. In fact, last year while at one home, I saw a jury duty notice for my wife in the daily Informed Delivery email for the other place. I could clearly read the juror number through the envelope, which was required in requesting a deferral online.

At the bottom of the Informed Delivery dashboard, there is a listing of tracking numbers for en route packages with their status, along with info about the sender if it's from a large shipper like Amazon or Macy's.

Again, thanks to "~Me" for an interesting and informative article.

Brobin

We suspect this is only the tip of the iceberg in uncovering fun facts about this program. Whether it's a convenience, a stalker's dream, or a means for authorities to keep track of all of your mail (or all three), we intend to have as much fun experimenting with (and trying to break) the system.

Dear *2600:*

Matt Muse's article in Spring 2020 about printers being a vector for data exfiltration is accurate. Having said that, the last several places I've worked (going back to 2013) have all had policies to configure printers so this doesn't happen. I have even run a project like that for 600 networked printers. I would never say that it is impossible to hack an organization through their printers; I'm not even close to that stupid or arrogant. But, it would be my assumption based on my experience that it's probably smaller companies (and larger companies with smaller-minded IT management) where this is still a problem.

Piano Guy

Dear *2600:*

Re "DoD on APN" (37:1), just a thought for ThoughtCrimes, I think both countries' military agencies have sold large chunks of those IP ranges, or returned them to the pool when IPv4 addresses were becoming scarce.

Keith

Dear *2600:*

In one of your most recent issues (36:4), I saw "thank you elliot" on the index page Why is it there? And also, I can't seem to access your store. All it said was "can not decode raw data." I don't know if it's just me or something else.

AJ

It must have been Elliot.

Dear *2600:*

Imagine how embarrassed we'd all feel if Facebook and Google had managed to get an editorial published in *2600* through a shill. Strangely, this happened in the Spring 2020 issue and is actually pretty obvious to anyone reading "Who Has Your Face" with even a little bit of skepticism. The article complains that state DMVs are releasing our photos to law enforcement agencies without our consent. While true - and concerning - the DMV has only one photo of me. It's over ten years old. I still had hair and little hipster glasses, and that would be an uphill battle for any face recognition algorithm today. In any case, my state, city, and county governments all actively limit police use of face recognition. You may be worse off if you live in Florida. But if people care, we can hold these institutions to account because, ultimately, they're public agencies and we control their funding.

Much more comprehensive datasets of your face that are much more outside your control are held by Facebook and Google. Would these loving corporations ever abuse your trust? They already have, as a trip to any search engine (try "Facebook face recognition") will reveal. Furthermore, the Facebook face database has been thoroughly scraped by an outfit called "Clearview AI." They're actively pimping all your nicely tagged faces to law enforcement, without public oversight and - more importantly - without the possibility of public oversight.

Amazingly, the EFF's article manages to complete ignore these facts, which are clearly a much more relevant threat to our privacy. Why would the EFF do that? Aren't they, like, the good guys? Actually, there was a remarkable expose about them in *The Baffler* a few years ago (thebaffler.com/salvos/all-effd-up-levine). It spells out in detail how, almost from day one, the EFF has been funded primarily by corporations, particularly Google and Facebook. The article describes many years of awkward logical contortions, remarkable blind spots, and aggressive lobbying to prevent tighter restrictions on corporate shenanigans with your data.

Maybe future articles by the EFF should be reviewed a bit more critically before publication? Or at least printed with one of those "Sponsored Article" headings.

RB in SF

It's great that you trust the government to play by the rules. We don't and it's doubtful we ever will. While holding them to account is nice in theory, when was the last time you saw that work in practice against entities like the FCC or DHS? It's a fantasy.

So we have this straight, your position is that EFF is being backed by these major corporations so that they'll take the government to court and curtail their privacy abuses, while opening up the door to even worse abuses by these same corporations? We don't buy it. (And EFF could not have been taking funds from Google and Facebook "almost from day one" as they were around more than a decade before either of those companies started to make their mark.)

Simply typing "Facebook" into the EFF's search bar will reveal titles like "Facebook's Arrogance," "Facebook's 'Evil Interfaces,'" or

Facebook's censorship under the microscope." They do not appear to be members of the Facebook fan club. Google admittedly doesn't have the same level of critique, likely because they haven't proven themselves to be as evil as Facebook, though there are certainly enough troubling signs for many to believe that it's only a matter of time. What EFF does is critique these entities when they get it wrong and praise them when they get it right. And while concern over where the money comes from has always existed, specifics over whether that affects their policy are what need to be focused on.

You will find that corporations tend to support civil rights organizations, even when their overall policies don't always align with those groups. It's a form of "brownie points" where they look good by supporting the right causes, but that doesn't necessarily mean the causes have become corrupted. Look at all of the major corporations that supported the Black Lives Matter movement and tell us you believe they will never be criticized by that organization if they engage in racist policies.

We are well aware of and very sensitive to those who turn a blind eye towards injustice and privacy violations when it comes from particular sources. In fact, we're seeing an awful lot of that in today's events. But we just don't see it when it comes to the EFF. And you've presented no actual evidence of its existence.

Discoveries

Dear *2600*:

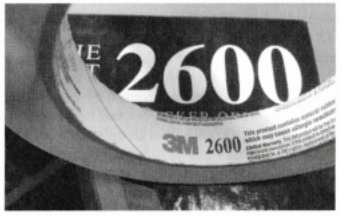
I have found that one can hide a micro SD card in the top of a payphone in between the lip of the lower/back housing and the upper/front housing. Also, placing the micro SD card on either of the farthest sides does a good job of securing it and preventing it from sliding in too far.

l00n

So now that we know how to do a payphone dead drop, all we need is a conspiracy.

Dear *2600*:

I'm not exactly sure where to submit this, but I found this roll of tape while putting up posters in a Latin class. The font is even a pretty good approximation of your own. Here it is with a *2600* collection for reference.



Erik

Yes, we've seen this before, but it's nice to know it's still out there. That is indeed our font. Perhaps we could make these rolls into promotional items of some sort. Who wouldn't want to have hacker tape?

Problems

Dear *2600*:

Hi, I want to change my membership mailing address. But I never made my account.

Jason

Letters like this really make it difficult to solve the problem. As we don't offer membership in anything, we assume you must be referring to a subscription to our magazine. And we're also going to assume that the account you're referring to is on our store, since we don't actually offer accounts. But the easiest and quickest way to change your physical address is to simply email us at subs@2600.com or call our office line at +1 631 751 2600.

Dear *2600*:

I hope you are doing well. I was ready to checkout on your website but couldn't locate the option to split up my order into smaller payments. I have used Amazon 5 Payments, Bread, and ViaBill in the past and was wondering if I could get a similar option on your website. Let me know.

Brent

It sounds like what you're looking for is a credit card. You're in luck, because we happen to take those. (Incidentally, we are not a credit card.)

Dear *2600*:

I hope everyone is doing well. I have a Google News subscription to the magazine and just wanted to see if this edition of the magazine is still getting updated. I cannot seem to see anything past October of 2019. Thanks!

Logan

You're going to be rather disappointed as Google decided we were no longer relevant to their vision of what publishing is. It's OK because we no longer think they're relevant to whatever it is they're trying to do.

Dear *2600*:

I am missing back issues of past *2600*s that I am subscribed to. Why is this?

Tim

We're going to make some huge assumptions here. We assume you don't want us to come to your home and investigate where your back issues disappeared to. You're not accusing us of somehow grabbing them back because our supplies ran low again. Finally, we're going to assume that you're talking about Kindle back issues since Amazon has a history of reaching into people's devices and erasing things, which we've asked them repeatedly not to do. But we've printed a solution to this in the past and will share it again here. Download a program called Calibre (calibre-ebook.com) and then download the DeDRM plugin (apprenticealf.wordpress.com), then load K4MobileDRM from the "Load plugin from file" option under Preferences>Plugins. Finally, you must convert them to EPUB so you can store them safely on the device of your choice. It's absurd that we have to go through this to save something we've already bought, but this is the nature of electronic publishing and we have absolutely no say in how it's run. We do, however, have the ability to let people know how to keep access to what they've already bought.

Assertions

Dear *2600*:

This is Anonymous!
We are Anonymous,
We are Legion,
We do not forget
We do not forgive
Expect us.

J.A.L.

Well, no one's ever sent us those words before. Signing your real name was a neat touch.

Dear *2600*:

I placed an order for a copy of *2600*. I do not consent to any use of my information as provided after my order is shipped as per your privacy policy. It's a bit ridiculous that this is an opt-out default and not opt-in, at *2600* of all places.

Marcin

Just what privacy policy were you looking at? Our says:

"We do not save your credit card information after your order is complete. We also do not share ANY of your information with anyone. If you've ordered a subscription, your name and address reside on our subscriber database which is located on a machine that is never connected to the net and which is protected by two levels of encryption that even the NSA would have trouble with. We will also NEVER send you unsolicited mail. In other words, we know a thing or two about privacy and we will do everything possible to protect yours."

We doubt you have a problem with that. Perhaps you're referring to the boilerplate Shopify and/or credit card policy which is standard everywhere and which we have no control over. We can only tell you what we won't do - we have no way of telling you what other entities you share your information with will do.

Aspirations

Dear *2600*:

Greetings and salutations the cyberverse it's been awhile since I last wrote to your fine publication 31:1 spring 2014 and I must say I've grown a lot since then thanks to informative and next gen resources such as *2600* and sans etc. as of lately I've been getting into the futuristic and simply bad ass concepts such as deep learning and cell site simulation and I was wondering if there are any projects out there involving deep learning malware which would be sweet think polymorphic self encrypting code generating worms. And home made Stingray devices using hack rf and Blade rf SDR technology look forward to hearing from you guys again.

your friend
THE ROCKET RIPPER

Periods are your friend. That's the first lesson. We look forward to your growing some more with a bit of trepidation.

Dear *2600*:

This is not a spam
This is not a spam.
I'm a new text block ready for your content.

Lauren

We've heard of identity crises before, but never anything like this. You're better than this, though. You're more than just a text block and don't let anyone tell you otherwise. At least you know you're not spam. That's always the first step.

Solicitations

Dear *2600*:

Hello there! I'm sorry to disturb you. I am a Chinese mask factory. There are a large number of disposable stocks. The masks have CE certification for the EU. In addition, the factory also has FDA and ISO certification. Welcome to contact us!

jklovetop

Uh huh. Now it's a factory with a sense of identity. Just what we need.

Dear *2600*:

I am an enthusiastic writer. While surfing the Internet, I found your site - https://www.2600.com/magazine/digital-editions.html that seemed to be very interesting and informative.

I would love to discuss an opportunity to create an article for you. My article would be custom made for your site and would be helpful for your readers.

Please let me know if this is something you would be interested in.

I look forward to your reply.

Best regards,

Shivani Parashar.

One of these days, we just have to take one of these people (or bots or whatever they are) up on their offer and see what we get. We love how they always pick some random page on our site, which apparently is supposed to impress us. (Our digital edition department was rather thrilled for a few minutes.)

Dear *2600*:

This is for those who can hack cryptotab or bitcoin and pay me for my job. I can download any files or app for those who are searched it. App for hacking or else, Actually I have Z Shadow. Those who need it, just send me message. And I can download you any app.

Dickson

At last, someone who can download apps for us.

We'd actually like to make a whole documentary following this person around.

Inspiration

Dear *2600:*

The way you are promoting the awareness of COVID-19 among people is quite amazing. You actually inspired us to take this a step farther and create something even deeper in the subject of novel coronavirus.

I thought I'd reach out to you because we just published a *huge* 21,300 word beast guide on COVID-19, which has gotten a great deal of attention lately. So I thought it's worthy of showing to you. The link is www.healthroid.com/conditions/covid-19/.

I'm pretty sure that you get some "noob" questions about COVID-19 now and then, so perhaps you'll find our guide good enough to share it with these people, instead of trying to explain everything on your own.

In this guide, we have covered everything your community needs to know about COVID-19 and even revealed:

- Four separate case studies of 44,909 confirmed cases in figuring out the exact pattern of coronavirus.
- The exact formula that China used to treat COVID-19 patients, with the help of which about 93 percent of total infected people have fully recovered.

And, all based on research and with sources to back it up.

Oh, and if you think our guide is lacking something, we'll be happy to revise it. So yeah, looking forward to your feedback. Either way, keep up the good work with *2600 Magazine*.

Priyank Pandey

We're pleased (and somewhat shocked) that we inspired this, and we're really happy that people are taking the initiative here to actually help people, something many of our leaders could take notes on. There are some other notable guides from our community. covid-at-home.info, foundry.bio/coronavirus-covid-19, covidbase.com, coronavirustechhandbook.com are a few. There are others and, as we hear of them, we'll pass them along.

Reflections

Dear *2600:*

I remember using computers in my childhood and seeing games bring me to life if I could wait for them to load. Sometimes I'd wait an hour.

I started using the Internet in 96 after reading your magazine and being awakened to war dialers. I always wanted to start scanning for interesting computers that way. Little did I know that one step forward into the Internet was all it takes to keep you there forever.

This was before video and audio were presented on the Internet. Technology was not there yet. I have to say that even my fight disappeared like a druggy's high. I was not scanning for numbers anymore. I totally forgot to fight the good fight. Foreign websites were all that I needed to fill the void in my life.

What I'm trying to say is that we started wondering if we could use a Cray or even better hack into one. Now all we do is get movies. I have since stopped and now buy them so I don't have to see morally questionable audio and video.

Keep up the good fight.

Bruce

You raise good points. Too much has been lost to consumerism and the magic of exploration isn't even on the radar of so many. But then again, was it ever? The Internet has brought everyone online, but the hacker mentality never really existed in more than a small fraction, regardless of the state of technology. There are lots of people who call themselves hackers because they've learned how to turn on a computer. We can assure everyone that there's a great deal more to it than that. We can also reassure those who, like you, are bemoaning the loss of something magical that the magic never truly disappears. It just changes its appearance. If it didn't, it would hardly remain magical in the first place.

Dear *2600:*

Hi how are you? I how to hack my near wifi router

HITESH BUNKAR

See, there it is. Magic.

Perseverance

Dear *2600:*

I'm 38 (whaaat) and literally have grown up with *2600*. I somehow stumbled onto local BBSes at a frighteningly young age (and laughably slow speed... 2400, then 9600 - the day I got a 28.8 modem was like the highlight of my adolescence). Anyway, it could have gone a lot of ways. Some would doubtlessly argue that the nascent wide-open expanse of cyberspace was no place for a 12-year-old girl, but I found my people there. I remember when I was little and desperate to see if anyone had software or systems I didn't have (I started out at age six or seven with my uncle's Apple II+ and boxes of mostly unmarked floppy disks - mostly games he and his friends had copied and shared - and literally taught myself everything I needed to know to make all of it mean something).

Point being, you can't stop now! I have layout experience and a wide array of additional skills, and I would be honored to volunteer to assist you guys with anything that you need to make sure that there is another issue... and another... and another. I can help with HOPE too. I don't need money - I'm making more now on unemployment than I ever made from working. Thanks coronavirus! And if you have ethical qualms about taking government funds, I would understand, but if not, I would suggest looking into some of those programs they have for small businesses. I have so many ideas and lots of time, but very few collaborators. It's all nothing without that.

marissa

We want to thank you and the many, many people who gave us words of encouragement and support when things looked pretty bleak. Those words, plus the remarkable comeback of what appeared to be a doomed HOPE conference due to a phenomenal show of support from attendees, is what makes this community so special, not only to us, but to people around the world who benefit from its knowledge and spirit. We had almost forgotten that.

Our troubles, of course, pale in comparison to what many others have been going through. That's why we all must turn attention to supporting one another regardless of any differences we might otherwise have. We could yet be facing the worst of this crisis and, while we have nothing but pride for how this community has reacted on so many levels, we are seriously worried about how our nation will come through this. All we can do is stand up for science when it's under attack and do everything we can to educate people so they don't fall victim to ignorance. The fact that we have to even write a sentence like that is horribly depressing.

Thanks again for your generous offer of help. We intend to stick around and fight for our existence. We hope everyone out there pledges to do the same.

Dear *2600:*

Been reading you guys off/on since the beginning. While I've tried to buy an issue whenever I see one on a shelf, these days I don't make it to many bookstores anymore.

I work at a large bank, and make an extremely comfortable living. I'm a high school dropout who's entirely self taught, and I owe a huge thanks to you guys for teaching me a way to think and how to learn. I hope you pull through this!

Aaron

Lately we haven't been making it to many bookstores either. The best ways right now to continue getting us is through subscriptions or our new online PDF version. We've lost a tremendous amount of sales due to all of the closures, but we could recoup those losses entirely if we gained thousands of subscribers through these means. And if we don't, we've got other options. We intend to explore them all. There are so many people out there who have yet to discover the magical world of hackers and will have their lives positively influenced by them, as you have. We feel we have an obligation to see that through. We hope you're able to encourage such people whenever you come upon them. And for everyone else, please, remember to support those businesses and places that you value. We've seen far too many disappear just in the past few months. We've learned how very fragile everything we take for granted really is.

Dear *2600:*

Good day, people of *2600!*

I wasn't sure which email address was appropriate for this, so I sent it to both this one and the webmaster address. I have been getting your magazine for about the last two and a half decades and was disheartened when I realized I would not be able to get your most recent issue at the bookstore. Realizing that I could get it from your website, I decided to pay the site a visit. I then read your note to your readers on April 15 about how much you all are struggling to make ends meet in the face of COVID-19. This saddens me. It got me thinking of ways to help. Without having a group of friends large enough to make a difference by simply asking them to purchase a magazine, I thought about crowd funding. Is this something you have considered? I was thinking about creating a GoFundMe page, or something along those lines, to raise money to Save *2600*. In fact, I would probably call it that. The issue with that, of course, is that I don't have the network to spread the message. If a page were created, is it something you would share on your Twitter? Obviously, I wouldn't go ahead with this without your blessing. If this is something you are already doing, or if you have another fundraiser going on, do you have a link I can spread to try and get the message out?

As I said, the idea of losing *2600* is a sad one. I have been a fan since I was introduced by my uncle almost 30 years ago at the age of 11. Your magazine was a driving force behind my interest in how technology works and is partly responsible for my going into IT. If there is any way for me to help, please let me know.

Thank you.

Jason

Thank you and the many others who wrote in with similar ideas. The thing is there are so many worthwhile causes and people who are truly suffering that we just wouldn't feel right asking for this kind of help. It's difficult, challenging, and infuriating, but in the end, we feel we'll figure out how to get through this. We live for the challenges, after all, though this is certainly one we could have done without. Getting our stranded issues into supermarkets was one creative idea we felt we had to try. And now we know that supermarkets are a terrible place for a hacker magazine. But rather than fixate on the failures, we're going to keep trying for success. And if it doesn't work, we'll adjust our expectations and other parameters. Financial problems are a pain, but what's worse is a feeling of hopelessness. And that, thanks to people like you, is something we don't think we'll

be experiencing anytime soon.

Dear *2600:*

I've been reading the magazine since my teenage years, and I've been on *Off The Hook* a few times. Been to a few of the HOPEs. I've always purchased my copy at Barnes and Noble, or ordered individual ones. However, seeing as Barnes and Noble is shut down and with all the uncertainty, I'm starting my subscription today. Please reach out to the community to make it through this difficult time. My children are getting to an age where I think they're ready to start reading as well.

Jim

Thanks for thinking of us. And if your kids are old enough to read, then they most definitely are ready to start reading us.

Dear *2600:*

I am where I am today because I read *2600* when it mattered. Please let us know how we can help; the infosec community loves you and will support you!

Matt

You bought a ticket to HOPE and we can't tell you how much that meant to us. It's that faith in us that made the issue you're reading possible.

Dear *2600:*

Is there is anything I can do to help HOPE and *2600* keep going? Please let me know. This magazine is so important. Stay safe.

Matthew

You're doing it right now. Supporting us, spreading the word, and keeping that hacker spirit going is all we could ask for. We've never been prouder to be part of this community. The way it's responded to the overall crisis is a model for all elements of society, one that we hope people everywhere take note of. Smart and conscientious people are the future.

Dear *2600:*

I was there two years ago and was not planning to come this year since it's not so simple from where I live (Europe). But I'm really looking forward to attending virtually. Great idea to adjust the format!

gamma gamma

We have to admit that we thought it was all over when it became clear we wouldn't be able to host the conference in person this year. But the spirit and confidence of people who had a vision and just knew that this was what people needed is what really turned things around for us. We wound up with a bigger response speaker-wise than ever before. And many of them, as well as attendees, had a similar conclusion to yours. Not having to worry about the travel and all of the hassles that go with that turned out to be rather liberating in a way. We had more content than ever from all corners of the world, representing so many different views and cultures. Truly, this turned into a Hackers On Planet Earth celebration. While this issue is being put together before the conference concluded, we've already seen such magic and inspiration that's come out of it. We hope it doesn't end there.

Dear *2600:*

I didn't plan on attending this year's conference, but someone forwarded the email the staff sent out regarding the financial issues HOPE and *2600* are having. I'm purchasing a ticket to support you guys. I know how difficult it must be. I'm also subscribing to the magazine too. You guys did a lot for me as a kid, allowing me to have a great InfoSec career. I'm glad I can pay you back in some way.

Good luck and thanks for everything you do for the community!

David
NC2600

We have to say, we never really appreciated how many people have been positively affected by us merely existing over the years. That alone is extremely gratifying. Thank you for your support and we hope you enjoy the conference!

Dear *2600:*

I have always appreciated *2600 Magazine* and how you support the phreak and hacker culture and community. Only recently have I truly begun to understand the editorial content. Thank you for everything you do, the least of which is continuing to publish this magazine through various dark times in the past few decades.

Ross

Yes, there have been a few dark times, haven't there? Let's hope this one is the darkest we have to experience.

HOPE 2020

[We had planned on having this issue finished well before HOPE, even with all of the delays and problems. But, since it wound up being pushed back even further, we actually had a couple of days after HOPE before we sent this issue to the printer. So we're including a couple of the early bits of feedback we received.]

Dear *2600:*

As an information junkie with a passion for lifelong learning and continuing education, I can't imagine a better way to have spent the past nine days than as a HOPE 2020 virtual attendee! This was a deeply enriching and invigorating experience.

HOPE 2020 was the great beacon of inspiration, encouragement, possibility, and yes - hope - that we all needed as we try to navigate a path through the dystopian nightmare of a runaway pandemic and a federal government led by the most incompetent, corrupt, and malevolent president in our nation's history.

Every speaker was uniquely inspiring and I'm extremely grateful to them all for generously donating their time to this amazing conference. I admire their impressive achievements and I'm deeply appreciative for the wisdom and insights they shared. I especially enjoyed talks delivered by BiaSciLab, Jamie Joyce, Bill Graydon, and Bruce Schneier, as well as workshops presented by Joe Gray, Brandon Roberts, Todd Schiller, and Mark Lam. I can't wait to binge watch all the talks I missed and re-watch every talk I attended.

Thanks to the dedication and commitment of a great volunteer team, years from now when I look back on this time in my life, it won't simply have been the summer of COVID-19 or the summer when a buffoonish, emotionally unstable president descended deeper down the rabbit hole of his own psychoses. It will have been *The Summer of HOPE!!*

As always, keep up the great work!

JK

We're happy to see that the material kept people thinking. It's easy to fall into a state of hopelessness (seriously, no pun intended) with all of the bad news lately. But we will get through it and we're all capable of a certain amount of impossible. Maybe that's a little clearer now.

Dear *2600:*

Just wanted to let you know, everyone at HOPE is doing a fantastic job - of course, I miss the (more intimate) social interaction. For what it's worth, you guys met tremendous challenges with tremendous success. Kudos! And thanks for all the hard work.

tmj

The hard work would have been fruitless were it not for the many attendees like you who were a vital part of the whole thing. It was a tough challenge, but our attendees helped to make it fun. Not to mention that your support helped keep the magazine alive.

Dear *2600:*

I am a not a skilled geek, but I am very glad I signed up for this conference. Can you help me figure out where the "sign-up codes" are for the workshops?

I also thought I saw that if workshops were full, we would be able to access them at a later time. Can you explain how to access them?

Thanks again for a very informative conference.

beth

(We got the info to her in time.) The workshops were far more popular (and plentiful) than we had planned. Our initial system of preregistering for workshops didn't work as well as we hoped, so we switched it around to make the whole thing more accessible. We got it right that time and the whole conference operated more smoothly on that level. We were expecting hiccups, but we managed to get past these ones rather quickly. Our attendees were extremely patient while we worked it all out.

Dear *2600:*

Talks aside (all of which that I've seen have been great), I really dig the constant conversation and interactivity of the Q&A room. That's a really neat way to get to experience a talk, and the moderators are doing an awesome job curating the questions for the speakers.

I had concerns at first about open chat rooms, but Matrix itself has been great. It's like reliving the old days of IRC with folks who are just stoked to be here instead of trolling. The late night HOPE war story chats are as close to being back on the Mez floor at 1 am as I'll get.

The live clock with the offset monitor playing footage between talks is extremely cool - definitely more of that. The user submitted bumps are a really cool idea as well.

NK

That makes us so happy to hear because that was where we worried the most. We wanted that community spirit to exist and to thrive. But any time you have interactive chats, there's a danger of it quickly devolving or of being overly controlled. Based on the overwhelming feedback from attendees (so far, at least), Matrix really seems to have come through in fostering an environment close to what we would want in real life. It worked particularly well with the Q&A sessions, where attendees wound up getting more access to speakers than would occur in a real life setting. The video clips (bumps) from attendees all over the world really added to the spirit and helped show some of the many places that HOPE was reaching.

Dear *2600:*

This was my first HOPE conference and *I absolutely loved it!* I cannot *wait* until the next one. You are all awesome.

Love,
Josh

Wow. Thanks so much for that. This whole thing really mushroomed into a major event out of the embers of the one we expected to put on. It just goes to show what hacker ingenuity can accomplish. We had a crew as good as any professional television network programming team and our various tech crews handled all sorts of challenges - anticipated as well as those unplanned for. And, of course, we had such incredible presenters who made the whole thing interesting for nine solid days. So there's lots of awesomeness to go around.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind.
As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99, Middle Island, NY 11953 USA

EFFecting Digital Freedom

by Jason Kelley

Be Wary of Surveillance Tech During the Pandemic

In just a few months, COVID-19 has dramatically shifted our relationship with our jobs, our families, our schools, and crucially, our technology. Its profound impact on how we use our devices and the Internet started almost from day one: with shelter-in-place and stay at home orders sending people into quarantine, many immediately began to rely more than ever on technology to work, learn, and share information and advice. And beyond that, its usefulness for dealing with the loss of in-person contact can't be overstated. Whether we're using it to create art, listen to music, organize, or just talk with friends, technology is essential during COVID-19.

But the relative ubiquity of devices such as smartphones has also meant that governments are considering how they might use this technology for large scale tracking of the general public, in the name of fighting back against the pandemic. And tech developers have been happy to suggest ways that they can assist in this monitoring. As with any sort of surveillance, it's important to weigh the risks and benefits carefully, even during a pandemic.

We ask three questions when analyzing proposals that would provide greater surveillance powers to the government: First, would the proposal work? Government has not shown that some intrusive technologies would be useful, such as remote thermal imaging cameras with a high margin of error. The second question we ask: would the surveillance excessively intrude on our freedoms? Dragnet surveillance cameras in public places that use face recognition are grave threats to our privacy. So is mounting such technologies on drones, or giving police officers access to public health data about where people who have tested positive live. We oppose such surveillance. And lastly we ask, does the technology come with sufficient safeguards? Sharing aggregate location data collected from smartphones, for example, should only happen if the data cannot be disaggregated to expose the personal information of identifiable people.

Much of the conversation around COVID-19 tracking has concerned two technologies: proximity tracking and location tracking. Both have been promoted as digital forms of traditional or manual contact tracing, in which healthcare workers interview an infected individual to learn about their movements and people with whom they have been in close contact. Healthcare workers then reach out to the infected person's potential contacts, and may offer them help, or ask them to self-isolate and get a test, treatment, or vaccination if available.

EFF opposes the use of location tracking in this manner. Proponents of this tech hope to determine which pairs of people have been in contact with each other by collecting location data (including GPS data) for all users of a mobile app, and looking for individuals who were in the same place at the same time. But this technology is not well-suited to contact tracing of COVID-19 cases because data from a mobile phone's GPS or from cell towers is simply not accurate enough to indicate whether two people came into close physical contact (i.e., within six feet) - but it is accurate enough to expose sensitive, individually identifiable information about a person's home, workplace, and routines.

Proximity tracking, on the other hand, uses Bluetooth Low Energy (BLE) to determine whether two smartphones are close enough for their users to transmit the virus. BLE measures proximity, not location, and thus is better suited to contact tracing of COVID-19 cases. When two users of the app come near each other, both apps estimate their proximity using Bluetooth signal strength. If the apps estimate that they are less than six feet apart for a sufficient period of time, the apps exchange identifiers. Each app logs the encounter with the other app's identifier. When a user of the app learns that they are infected with COVID-19, other users can be notified of their own infection risk.

While Bluetooth proximity tracking is the most promising approach so far, it needs rigorous security testing and data minimization. For example, there is some risk that people can collect Bluetooth tokens, and use those to learn when certain people report their infection status.

Also, it is unclear whether proximity tracking will work. If it does, it will be at most a secondary part of our public health response. No COVID tracking app will work without widespread testing and interview-based contact tracing. Any app-based or smartphone-based solution will systematically miss groups least likely to have a smartphone and most at risk of COVID-19; in the United States, that includes elderly people, low-income households, and rural communities. It will also systematically ring false alarms, for example, when people within six feet were separated by a wall.

Ultimately, no one should be forced to use proximity tracing. We need laws protecting people from coercion to use one of these apps, including a ban on discrimination in employment and public accommodations against people who don't use them. Also, many new COVID-era government surveillance programs are being built in partnership with corporations that hold vast stores of consumers' personal data - which shows the need for new laws to protect our data privacy.

There are other technologies that can help address the public health crisis that aren't getting as much attention, but should be: we must have free and open access to scientific knowledge about the virus, and tinkerers should be able to fix and repair medical devices with a strong right to repair. Also, the federal government should exercise its power to stop patent trolls from endangering COVID-19 testing and treatment, and should not increase patent terms for technologies related to this health crisis.

This pandemic is an opportunity for us to rethink our relationship to technology. We must empower people to take control over their devices, and to appreciate the good that they can do while identifying the danger. This is a moment for us to recognize both the promises and the pitfalls of our relationship with our technology, and to draw the lines between utopia and dystopia more clearly than ever before. If we do it right, we can emerge from this time with our freedom and democracy as strong, if not stronger, than when we went in.

Fun with Text to Speech

by Nestor

I just purchased the *2600 Hacker Digest*, Volume 35. This time I decided on the EPUB format because I have noticed that using Calibre, EPUB converts rather nicely into text. After downloading it, I promptly converted the EPUB into plain old UTF-8 text and started reading. Very soon it occurred to me that I was running late and must stop reading. It was getting into the afternoon and I had other things I needed to catch up on. What was I to do? I was just settling into reading and now I had to stop. Fooey!

Well, as a little experiment, I decided to try rendering portions of the file as text to speech. I have a little pet project hosted on GitHub, which is a rehabilitated version of a public domain speech synthesizer named PicoTTS, which I lovingly renamed to NanoTTS. My whole contribution really is that I took the PicoTTS code, which was not functioning when I found it, and made it into a functioning command line tool with sensible commands and options, coupled with a few different choices for outputs.

NanoTTS supports six different voice synthesis modules: en-US, en-GB, de-DE, es-ES, fr-FR, it-IT, as well as allowing several different options which affect inflection, such as dialing in the speed of the reader and the pitch of their voice. I tried this in the past to varying degrees of success, but thought this time I would attempt it once more so I could keep reading *2600*, even though I was busy doing things. And wouldn't you know it - it worked wonderfully this time.

My first decision was, instead of converting the entire *2600* digest into a single, huge audio file, I decided to carve out little chunks of the file - one article at a time - and convert each of those into WAV files. Surprisingly, in relatively short time - and using Bash no less - I was able to generate MP3s for the entire digest. What surprised me most of all is that the output is surprisingly listenable. I think I actually can understand everything the reader is saying. This is no small feat, given how wooden and awful synthesized voices often sound. And this one isn't the greatest either.

For anyone who wants to convert the entire *Hacker Digest Volume 35* into nicely labeled audio snippets, you need four things: 1) *2600 Hacker Digest, Volume 35* in EPUB format; 2) Calibre (which you use to convert it into TXT format - make sure UTF-8 is selected in the output options! This is the only option I checked. I left the others alone. For instance, don't turn on Heuristic processing.); 3) NanoTTS, which you can get from GitHub at `github.com/gmn/nanotts`;4) lame MP3 encoder.

Please note that I have actually added this script to the NanoTTS GitHub repository in its entirety. If your EPUB converts producing identical TXT output as mine, you should be able to run the script out of the box without altering anything. It will generate the entire set of audio files in the current directory.

The code works simply by taking a list of line numbers. The line numbers come in pairs: the first is the line to start on, the second is the line to end on, both are inclusive. You can check this by opening the text file and verifying a few visually. If the first couple match, there's a good chance they all will. But in order to be really sure, here is the SHA-256 of the text file: `eee2f06df21436fdb374935f➥c7fd2d1e8384c9afe4c6f5ae1c3c➥bf0e8efdd1ae`. We merely iterate through the line-pairs and run NanoTTS for each snippet, generating an MP3 file, and voila, we can turn an entire magazine into actually listenable audio for those busy folks on the go who might have to drive somewhere, or mow the lawn like me.

Enjoy!

```
#!/bin/bash
# Convert the entire digest
➥ issue of 2600 volume 35 into
➥ audio files for easy listening!

# I have found these settings
➥ considerably improve the
➥ legibility of the nanotts
➥ output; ymmv
speed="0.8"
speed="0.78"
voice="en-US"
volume="0.6"
pitch="1.14"
```

```
# your file location and name will vary, obviously.
FILENAME=../../documents/2600_MAGAZINE/2600_\ The\ Hacker\ Digest\
➥ -\ Volume\ 35.txt

# Even though it may not look like it, these numbers are in pairs;
# Each pair is a starting and ending line (inclusive) of a section
➥ of text
SECTIONS="204 224 230 264 270 328 334 462 468 594 600 648 654 782
➥ 788 892 898 988 994 1006 1012 1048 1054 1124 1130 1160 1166 1194
➥ 1202 1222 1228 1254
 1260 1300 1306 1374 1380 1542 1548 1582 1588 1632 1638 1652 1658
➥ 1688 1694 1748 1754 1832 1838 1862 1868 1950 1956 1990 1998 2126
➥ 2132 2164
 2170 2236 2242 2312 2318 2342 2348 2384 2390 2452 2458 2568 2576
➥ 2630 2636 2676 2682 2698 2704 2840 2846 2874 2880 2906 2912 3046
➥ 3052 3112
 3120 3144 3150 3172 3178 3204 3210 3300 3306 3472 3478 3518 3524
➥ 3548 3554 3602 3608 3634 3640 3678 3684 3740 3746 3884 3890 3926
➥ 3932 3972
 3978 4000 4006 4128 4134 4166 4172 4244 4250 4272 4278 4316 4322
➥ 4360 4366 4426 4432 4462 4472 5192 5200 5230 5236 5322 5328 5354
➥ 5360 5480
 5486 5504 5510 5536 5542 5564 5570 5592 5598 5610 5616 5630 5636
➥ 5656 5662 5806 5814 5832 5838 5880 5886 5908 5914 5930 5936 6046
➥ 6052 6776
 6780 7438 7442 8088 8092 8796 8882 8898 9692 9754 "

COUNT=1
HEAD=''
TAIL=''

function run_nanotts() {
 local count=$3
 local title="$4"
 while [ ${#count} -lt 3 ]; do count=0$count; done
 local file="$count-2600_vol.35-$title.mp3"
 echo "nanotts --speed $speed --volume $volume --pitch $pitch
➥  --voice $voice < <( head -$1 \"${FILENAME}\" | tail -$2; echo "
➥ . . . . . " ) -c | lame -r -s 16 -m m -V 0 -b 56 --ta \"2600
➥ Magazine\" --tl \"2600 Vol. 35\" --tn $count - \"$file\""
➥>/dev/stderr
   nanotts --speed $speed --volume $volume --pitch $pitch --voice
➥ $voice < <( head -$1 "${FILENAME}" | tail -$2; echo " . . . . .
➥ . " ) -c | lame -r -s 16 -m m -V 0 -b 56 --ta "2600 Magazine"
➥ --tl "2600 Vol. 35" --tn $count - "$file"
}

for sect in ${SECTIONS}; do
 echo $sect >/dev/stderr
 if [ -z "$TAIL" ]; then
  TAIL=$sect
 else
  HEAD=$sect
  let TAIL="$HEAD-$TAIL+1"

  echo "head -$HEAD "$FILENAME" | tail -$TAIL" >/dev/stderr
     head -$HEAD "$FILENAME" | tail -$TAIL
  echo >/dev/stderr;

  TITLE=`head -$HEAD "$FILENAME" | tail -$TAIL | head -1`

  run_nanotts $HEAD $TAIL ${COUNT} "${TITLE}"

  HEAD=''; TAIL=''
  let COUNT="$COUNT+1"

  sleep 3
 fi
done
```


HACKER EMAIL

by Sh0kwave

Hackers and other privacy minded individuals use Protonmail (protonmail.com). It is hosted in Switzerland to take advantage of Swiss privacy laws, and is encrypted end to end. Go on the dark web and you will see that a lot of contact email addresses are protonmail.com.

You say you haven't been on the dark web? Why not? Get a Tor browser and a personal VPN and check it out. Why do you need both? Using the Tor network will get you anonymity, but does not guarantee privacy. It will hide your source IP address, but if you visit a site outside of Tor your traffic is not necessarily encrypted. VPN will give you privacy (encryption), but not necessarily anonymity, which is why you should use both. Be careful, not all VPN providers are the same. You want one that does not maintain any logs, or they might turn over their logs of your activity to law enforcement if asked.

Back to email. Two other services you should be aware of are Mailinator and Guerrilla Mail. These are similar, but have a few key differences. If you are being asked by a product or service to provide an email address so you can receive an activation link or code (and you know this will generate a never ending flood of spam in the future), give them anything-at-all@mailinator.com. When Mailinator receives an email from anywhere with any name, it instantly creates that mailbox and keeps it around for about an hour. It is not private. In fact, there is no security. Anyone who knows the name of the mailbox can read the contents. You could try to give your mailbox a "tricky name" but that is security by obscurity, and it is not a good idea. And that is not what Mailinator is for anyway. It is disposable email, or burner email, just for one-time use type activities. And, an important point, it is receive only.

The fact that you cannot send email from Mailinator is why you might want to use guerrillamail.com. It is similar to Mailinator in that you can send mail to it with any name and a mailbox will instantly be created for about an hour. But you can also send from Guerrilla Mail. You can also pick your own address to send from, and there are multiple domain options to use. Very rarely I have used Mailinator and the email was deemed not valid or blocked by the service or product I was trying to validate. However Guerrilla Mail gives you some choices. How about 1337hacker@sharklasers.com? Or spamdump@pokemail.net? You can create these. You can send to a single email address, no CC or BCC allowed. (So you cannot use it to generate your own spam.)

Mailinator and Guerrilla Mail can be handy, but remember they provide no security and no privacy. If you want that, use something like Protonmail. And it you are really, really serious, use it with a Tor browser and a VPN provider that does not keep logs.

Cerebral Spill

by Worlds_Gr8test_Defective

I am calling for an Information Revolution. Gone are the days in the United States of America where you can turn on the evening news and be presented vetted facts based on the most significant events of the past 24 hours. Instead, we have a 24 hour for-profit news cycle spitting out half baked, emotionally loaded, biased information in an attempt to attract viewers.

Televised news is not the only guilty party. The Internet has grown from adolescence and made amazing strides in providing people with avenues and resources for analyzing a diverse plethora of information, along with a diverse population to have conversations. However, this too continues to be tainted with information manipulation and for-profit schemes to attract viewers on websites loaded with ads also based on targeted advertising.

We have become more connected yet grow further apart in large part due to information manipulation. When facts don't matter and reaffirming your own preconditioned biases becomes a priority, we have failed as critical thinkers.

In an age where we are approaching the vectors of automation and robotics being used to replace human beings, it becomes harder to argue against this when we prove time and time again how easy it is to suppress our ability to analyze, investigate, and correlate. When a human brain does not exercise its ability to do these things, then tell me... what is the difference between that and a playwork written into lines of code?

I have learned stumbling throughout my life to never present a problem without also having at least a framework to move towards a solution. For this I recommend offering courses starting in elementary/primary school that teach media literacy. Not just teaching how to cite sources and correlate information, but also detection of biased or emotionally loaded reporting, as this is often the first indication of attempting to distort and manipulate a narrative.

I wish this was an original idea from my mind, but it's already in action outside the United States. Finland is an example of how teaching media literacy as a deliberate and collectively supported educational method has already produced positive results. The United States already has private organizations in place that have a vested interest in making progress towards media literacy. However, this has proven to not produce substantial results and lags behind in collective priority compared to international counterparts. The Department of State's Bureau of Public Affairs has also executed an initiative to work towards factual reporting, but there are checks and balances in place for the government to regulate this.

I am not advocating for government regulation or the banishment of independent privatized media. I want a collective understanding that information is powerful and, if not properly analyzed and digested, can lead towards destruction. A successful democracy can only flourish when your citizens are educated and informed. We have amazing minds capable of amazing ideas; please do not allow others to take away your inherent freedom of thought.

Sources for Further Reading

www.state.gov/media-literacy-and-combatting-disinformation/

www.pbs.org/newshour/politics/social-media-disinformation-leads-election-security-concerns-poll-finds

medialukutaitosuomessa.fi/en/

OhNoDaddy: GoDaddy Compromised

by Lg0p89

Everyone knows of GoDaddy (www.godaddy.com) and their services. Years ago, the business became a household name with their commercials. Since this time, the business has grown and become a bit more conservative, as evidenced by their website. This growth has made GoDaddy the world's largest domain registrar with 19 million customers, seven million managed domains, and millions of hosted websites. In comparison to GoDaddy's peers, this is huge.

Breach

The short summary is that there was a data breach focused on the web hosting account credentials. This is a rather serious issue for GoDaddy. With the amount of data held with the credentials and other confidential information held by GoDaddy from their clients, the targeting was no surprise.

The breach came to light in an indirect manner. The breach itself was not identified, but odd activity was detected on a portion of the GoDaddy servers on April 17, 2020. Six days later on April 23, 2020, the customers affected were identified.

The breach itself allegedly occurred on October 19, 2019, or over six months earlier, per the State of California Department of Justice. A notice was filed per the California Civil Code section 1798.29(e). This was disclosed by GoDaddy on May 4, 2020. The business only published and began to inform the affected persons in early May.

This was confirmed by Demetrius Comes, the CISO and vice president of engineering.

Method

Naturally, GoDaddy initiated an investigation. The parties concluded that the unauthorized person acquired the login credentials. This meant they could connect via SSH for the compromised accounts. The access makes the attack specifically useful. Until the password was reset, the least the attacker could do would be to modify the websites with profane language, or inappropriate images.

Scope

Fortunately, this did not affect all the accounts. It did affect approximately 28,000 customers. This affected only the hosting accounts and did not involve the customer accounts, main GoDaddy.com customer accounts, or the personal information held within these. They do note, for what it's worth, that it does not appear any files were modified or added to the affected accounts. They were not able to definitely state if any of the files had been viewed or copied though. The latter is really where the issue is focused. If the files had been modified, this is clearly not a good thing. Since the business doesn't know if they were viewed or copied, the conservative view is that they were at least viewed and should be treated as such.

Mitigations

The business did take the conservative route, fortunately, and presumed there was the access. To remove future issues on this specific point, the affected hosting account logins were toggled to require a reset. To assist and answer questions for the customers so that the help line was not inundated, an email was sent to the affected customers directing them to log in, giving them the procedures to follow. Without the reset, the customers would not have access to their hosting account. GoDaddy also, as a follow-up, had the customers audit their hosting accounts for any anomalies. One possibility was that admin accounts were created by the unauthorized attacker.

When Will This Be Over?

While the incident began over six month earlier and the forensic work had been mostly completed, the investigation continued. While it does appear that GoDaddy's actions halted the attacker's potential for access, GoDaddy is continuing to evaluate the breach's effect across its environment. GoDaddy is not releasing much other information than what has been published already, unfortunately. The disclosure would be useful, as the other persons in the industry could learn from this.

Issues

Indeed, the breach on its own is an issue for obvious reasons. There are other significant and legitimate concerns though.

One of these is the fact that it is not known how many customers actually are aware that their web hosting account credentials have been compromised. This is a problem in that while the affected GoDaddy customers are unaware of their credentials floating through the Internet we know and love, these may be used for malicious activities. In theory, if they wanted to bother the customers, they could log in, change the credentials and other information, and make it very difficult for the authentic owner to log into their account, unless funds were to exchange hands. They may also access other information which they could use to the real owner's detriment.

To investigate these matters certainly takes a significant amount of time. The evidence would be sparse and possibly spread among different systems, and difficult to correlate. The well-versed attacker would also attempt to remove their footprint from the attack(s) to further complicate the detection and forensic work. With all the factors combined, this is not such a simple task. Bearing this in mind, GoDaddy should have detected this well before the end of April 2020. Perhaps their SIEM (Security Information and Event Management) should have picked up some form of anomalous activity prior to the over six month mark. Having customers' private information on sale or possibly being used for other unauthorized purposes is not acceptable. Once the baseline breach information was accumulated and work done forensically on the system, the users should have been notified. Granted, this should not have been immediate, but it should have been done at the appropriate time. It appears that this time was extended for some reason. Possibly the business wanted to be conservative and wait an extended period in the hope that other evidence would come to rise. Instead of attempting to balance this, the customers really should have been notified earlier.

GoDaddy is offering a year of complimentary security and malware removal for the affected customers, which it should. A year, though, is a minimum amount of time. If I were the attacker, I now know what the benchmark is and would game the system with starting the individual attacks a year and a few days later.

Trend?

This isn't the only oversight reported in this period. On March 31, 2020, the illustrious yet distinguished Brian Krebs reported a GoDaddy staff member was a victim of a spear phishing attack. The attack, post establishing a foothold, pivoted and successfully attacked a limited number of other GoDaddy domain customers.

Last year also, attackers used hundreds of compromised GoDaddy accounts to create 15,000 subdomains. A portion of these were designed to impersonate popular website accounts or to redirect possible victims to spam pages. Earlier in 2019, GoDaddy was inserting JavaScript into its U.S. customers' websites without their authorization.

In 2018, GoDaddy publicly exposed high-level configuration data for tens of thousands of systems in AWS. This was due to a cloud storage misconfiguration.

Book Review

***The History of the Future: Oculus, Facebook, and the Revolution that Swept Virtual Reality*, Blake J. Harris, Dey Street Books, 2019, ISBN 9780062455963**

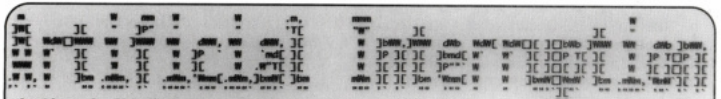
Review by paulml

Over the past 20 or 30 years, virtual reality has become something of a joke. Many companies promised that they would be the one to make it a reality. All have failed. A California teenager named Palmer Luckey was determined to do something about it.

In 2012, he turned the trailer he was living in, sitting in his parents' driveway, into a VR workshop. Teaming up with legendary game designer John Carmack, early demos of the headset were very favorable. Gathering a colorful group of fellow employees, they decided on Oculus as a company name, and thus began the usual entrepreneurial journey of ups and downs. Reactions to the Oculus headset from those who tried it continued to be very favorable (the phrase "game changer" was a common reaction). Their Kickstarter campaign was very popular.

The company was eventually sold to Facebook for more than two billion dollars. The reaction among many in the hardcore gamer world was outright hostility. In 2016, Luckey did something very normal and reasonable (and very legal) that created a public relations firestorm. Luckey became the most hated man in America. Things did not end well for him.

This is a wonderful book. For anyone who has ever dreamed of virtual reality, this is a must read. It also works really well as a purely business book. Maybe virtual reality's time has (finally) come. This is very highly recommended.



by Alexander Urbelis

Corporate Greed and the Pandemic

As regular *Off The Hook* listeners will recall, I've been living outside of New York City at my lake house in the Poconos Mountains of Pennsylvania. There are far worse places to be and we are incredibly fortunate. *Unfortunately*, however, while hunched over a kayak on a hot and humid day attempting to fix a seat clamp, my iPhone 8 Plus slipped out of my pocket, through an opening on the wooden deck, and fell face-down directly into a pointed edge of a large boulder.

I had faith. I've had this phone for several years and it's never quit. But this time was different. Flickering and rolling like a VHS tape with the tracking off, the screen was shattered beyond usability. And the phone likely took in some water, as there was a translucent, glowing ooze of significant viscosity slowly making its way around the screen.

I was pissed. But I could not at that moment have predicted the anger I would have for T-Mobile in less than 24 hours.

In the middle of HOPE and with a busy week of client calls on the calendar, I needed a new phone. I was stuck with a T-Mobile business plan and the nearest T-Mobile store was a 40 minute drive with the store closing in less than two hours. I could make it.

The store, however, was in a mall and I had barely ventured into indoor spaces for the past five months. Candidly, I was a bit freaked out at having to go to a mall, but had to brave it if I wanted to resolve the phone issue.

Everything felt strange. The whole idea of this mall space felt out of place. A tuxedo shop with a faded sign seemed like a relic from a bygone era when humans gathered at the slightest provocation to recklessly and irresponsibly celebrate things like weddings, graduations, or being granted some award or honor. The small kiosks in the corridors that sold mobile phone cases, earrings, sunglasses, that sort of thing, had no customers. The kiosks were mostly open but the people manning them looked like they were there because they had no other option. The whole place was sad and depressing.

I got to the middle of the mall, apparently shaped like an addition sign. From this spot there were four pathways. Having come from one of the directions, the T-Mobile store could have been in any of the three other directions. I took a left. These guesses usually never work out for me. In fact, in situations like this when I feel like something is in one direction, I usually go the opposite way on the assumption that my gut sense of direction is most probably wrong. Shockingly, the T-Mobile store appeared.

There were only two employees, both of whom were engaged with other customers. After smelling my own breath for what felt like 90 minutes but was probably more like ten, it was my turn. I explained the predicament. I said I was sick of the phone rat race and wouldn't mind another iPhone 8 Plus because it did the job and took great pictures. That was met with a short tut and a long explanation that the iPhone 8 had been discontinued years ago, and that I could search used electronics stores if I wanted that model. The iPhone 11 was my only choice. "Fine," I said, "I'll take it in the flashy Ferrari-like red and I need the 265 gig model since I'll be restoring from a backup of about 180 gigs." I was then informed that they only carried models up to 64 gigs in-store, and anything over that capacity would have to be mailed to me, arriving usually within three days or so.

This was an annoying revelation because it meant 1) that I would be without a phone for another three days and 2) that this whole fiasco of going to the mall and the T-Mobile shop itself was entirely unnecessary. If I'd wanted to wait several days for a phone, I could have easily ordered a replacement online. "Fine," I said and forked over my credit card that T-Mobile charged for over $900.

I left the mall feeling pissed off and ripped off. But again, I could not at that moment have predicted the anger I would have for T-Mobile in less than 24 hours.

After another 40 minute drive back home during which I cultivated the feeling of being pissed off and ripped off, I was determined to see if there were any places nearby where I could repair an iPhone screen. Lo and behold, I found one. Upon examining the address, it appeared to be located within the very same mall from which I just came.

I called them. They answered. They informed me that, yes, they were in the same mall and that in fact they were a mere fifteen feet away from the T-Mobile store. In stark contrast to the T-Mobile service I received, these guys were friendly, knowledgeable, and helpful. And to boot, they showed up at my house that evening, fixed my iPhone 8 screen in the driveway in less than 20 minutes, and charged me less than one tenth of what T-Mobile did for a new phone.

Sorting this all out in the course of an evening, I felt a sense of accomplishment. Things had gotten done. All I had to do was call T-Mobile the next day and cancel my order. Things, however, are never that simple.

I called T-Mobile the next morning. The wait was over 30 minutes, so I elected for a call back. T-Mobile called me at the most inopportune time - getting the kids the in the car - and put me through a Gestapo-style verification of personal details. Then I had to relay the details of the order, what it was, where it was placed, when, why I was canceling.... After this mini-deposition, I was placed on what was promised to be a 'brief' hold. Many minutes later, the customer service representative surfaced and nonchalantly and politely relayed to me T-Mobile's decision. Our repartee went something like this:

"I'm sorry, but we are not going to be able to cancel your order over the phone."

Mouth agape and brain misfiring, all I could get out was, "Excuse me?"

"We cannot cancel your order over the phone. If you want to cancel your order, you will have to go to the T-Mobile store where you made your order to cancel it."

This was the zenith of my anger with T-Mobile.

"Are you kidding me? The order is less than 24 hours old. The store is 40 minutes away and within an indoor mall. And, by the way, did you forget that there is a global health crisis right now?"

I explained the obvious: forcing me to travel to a T-Mobile store, which is an indoor space within a mall, thus an indoor space within an indoor space, was dangerous, reckless, and against all health and governmental guidance to combat the pandemic.

The representative expressed a bored apology. I expressed outrage which, of course, made no difference whatsoever. Like a customer service martial artist, the representative was ready for my next move without flinching.

"I'd like to speak to a supervisor."

"None is available," he replied.

It was the outset of HOPE. I took to Twitter to complain and detail this absurdity, tagging it with '#hopeconf'. People expressed outrage and the T-Mobile-social-media-disaster-prevention-and brand-protection-special-operations-A-team sprang into action. I received several public messages saying T-Mobile wanted to help and, to help them do so, I should direct message them.

This ended fruitlessly after I messaged their customer service rep and found out that I would need to connect my T-Mobile account, a business account, to my personal Twitter account. Given how my law firm is engaged in sensitive matters and combats APTs (Advanced Persistent Threats), connecting my Twitter account to our firm-wide mobile account seemed like a great way to get SIM-jacked.

I had no choice but to wait for a supervisor to call me back. One day later, I received a notification that the new phone I ordered (and was desperately trying to cancel) had shipped. About 30 minutes later, T-Mobile called. We went back and forth a bit and they agreed to cancel the order without requiring me to return to the physical store.

I explained to the supervisor that an outside observer looking at this transaction could reasonably conclude that, perhaps, T-Mobile's policies were deliberately designed to exploit the fear of traveling and contracting the coronavirus so that the company could hold onto a few more dollars than it otherwise would. I was then informed that I would need to return the phone they had already shipped or be billed for it.

Using the DNS intelligence platform I created, this experience provided me the impetus to see how many domains with the strings "tmobile" or "t-mobile" together with the string "sucks" existed. Not surprisingly, there were quite a few. NS records indicated that out of the 20 domains in existence, T-Mobile itself owned five. But, to my chagrin, none of the 20 domains resolved to anything other than pay-per-click advertising.

Like video killing the radio star, my theory is that social media has killed the art of the gripe site. However, just as MTV elevated untold numbers of musicians to cult status, so too can the gripe site leverage social media as a springboard. I will be reporting back on this phenomenon - and any others within and without the DNS - in the months ahead.

Until then, keep wearing your mask, if for no other reason than (as we learned at HOPE) masks present significant difficulties for facial recognition systems.

WASH YOUR HANDS
WEAR A MASK
READ 2600
(we'll get through this)

The Rise of the Machines - Learning to Detect DGAs

by blodgic

The cat and mouse game in cybersecurity of blocking attackers based on a domain or IP address is archaic. In the ever-growing realm of bots and command and control architecture, domain assignments have shifted from fast flux, a node shuffling method of DNS and compromised hosts, to a method called Domain Generation Algorithms (DGA). Block and tackle defense on DGAs is costly, but with a proper implementation, machine learning detection can be fruitful.

The DGA technique produces a list of constantly changing domains from a randomized seed of code. This code and seed create a rendezvous point between a command and control server and the infected client. If a domain is blocked, resiliency is built in and a new domain can be used to bring back the bi-directional traffic between the host and the C2 server.

The DGA domain is made of random numbers, letters, and characters (example: qx44utti3xbiz74hw2v5owww.net). In addition to a resilient communication channel, it is also a masquerade and evade tactic. Because the domain does not look like a word or group of words, and it's usually newly registered, it can evade proxy categorization. Your typical email clicker may also be curious to the site behind this strange gathering of characters. With this lure and evasion, the DGA trap is set and the attack technique has spun another web of deception.

To defend against this attack, blue teams thoroughly investigate and diagnosis nefarious network activity by blocking connections to the known IP address or domain of the C2 server. Even though the blue team blocked the traffic, if the malware was not properly removed, the same nefarious network connection originating from malware installation continues because it has spun up a new domain and the connection link continues.

This DGA scheme has been around since 2008 with Kraken. DGAs found huge success later in 2009 with the Conficker worm. Ransomware has since picked up the DGA technique and, well, ransomware is continuing to do its thing.

So why not fight fire with fire? Or, in the case of defenders, use an algorithm to defend against another algorithm. With the availability of labeled data, open source intel, and feature engineering, the DGA detection use case has a lower barrier to entry for an ML application. Rather than put together blacklists of known DGAs, an ML algorithm can predict and classify a DGA domain to aid in thwarting the attack.

The development lure of using DGAs originates from a seed function that creates randomness in domains. The seeds for DGAs vary and have been found by malware researchers to range from today's date, the trending hashtag on Twitter, the temperature in a city, and the exchange rate between two countries. This randomness has caused havoc for defenders and security researchers to develop defense techniques to counteract it.

To complicate defense further, domain registers are stimulating this random domain creation by allowing automated and anonymous registration. In retrospect, security researchers have done a tremendous job reverse engineering DGAs and labeling it to a malware family. This labeling is extremely helpful to data scientists as it provides classification labels to be used in prediction.

Building an ML DGA Detection Algorithm

Curating a list of domains is the first step in obtaining training data for a supervised machine learning model to combat DGAs. A binary label for each domain is assigned. We will give a 0 label for benign domains and a 1 for DGA domains.

Where to Get Training Data for DGAs:

DGAs

- Netlab 360 DGA feeds
- Bambenek Consulting

Benign domains

- Alexa top one million
- Cisco Umbrella top one million

Pulling down the DGA intel sources above should give you a list of more than a million unique DGA domains. A proportion size of 3:1 (three benign domains to one DGA) is an appropriate assignment to get a realistic prediction accuracy. The next step is to breakout each domain and try to build features that attribute it to being more closely aligned to a DGA.

At this point we have to get creative and itemize how we as humans infer how a domain looks more like a random set of letters and numbers. Feature engineering will give this inference or code to a machine to interpret our human resemblance and provide back a probability of a domain's likelihood of being a DGA.

There are Pythonic utilities to help us build features on domains like the domain parser, tldextract, and a word parser, like the wordsegment library. Wordsegment has fascinating capabilities with its trillion-word corpus that can dissect a full string and break out words into a dictionary. These packages ease feature engineering which would otherwise incur writing a ton of code.

Now that we have a domain broken out in words, segments, and its TLD, we will still need to conduct further feature engineering to get us closer to a machine learning model that predicts DGAs.

One step to determine randomness of a character in a domain is to measure its entropy. Entropy is a mathematical measurement of uncertainty in a random variable. The more random a string is, or the more uniqueness of letters, numbers, and characters in the string, the higher the value of entropy.

For example, a DGA of OLKQXMAEUIWYX[.]XXX has an entropy score of 3.40 and google[.]com gets an entropy score of 2.64. If we were to boil this down in cybersecurity economics, a higher score in randomness or entropy results in a higher likelihood of identifying a DGA.

Our feature engineering journey continues in the Python code below. This code implies that a Python pandas data frame or "df" was created for the benign and DGA domains. This data frame of domains will also include a target variable column or, in a statistical formula, the "y" and the binary label (DGA-1 versus Benign-0). The data frame will get wider and include more columns once you start adding more features.

These tactics on their own can be effective in identifying DGAs. However, it is the combination of multiple features bound together with a prediction function that will warrant more success in the prediction of DGAs.

Other assumptions for this example code below include importing the python package's math, sklearn, and XGBoost.

```
#python version 3.6
#DGA feature building

#entropy
def entropy(string):
  #get probability of chars in string
  prob = [ float(string.count(c)) / len(string) for c in
➥ dict.fromkeys(list(string)) ]
  #calculate the entropy
  entropy = - sum([p * math.log(p) / math.log(2.0) for p in prob])
  return entropy
#apply entropy to the domain
df['entropy'] = df['domain'].apply(entropy)
#Additional features

#hyphen count
df['hyphen_count'] = df.domain.str.count('-')
#dot count
df['dot_count'] = df.domain.str.count(r'\.')
#string length of the full domain
df['string_len_domain'] = df.domain.str.len()
#tld length
df['tld_len'] = df.tld.str.len()
#count of vowels and consonants
vowels = set("aeiou")
```

```
cons = set("bcdfghjklmnpqrstvwxyz")
df['Vowels'] = [sum(1 for c in x if c in vowels) for x in df['domain']]
df['Consonants'] = [sum(1 for c in x if c
in cons) for x in df['domain']]
#consonents to vowels ratio
df['consec_vowel_ratio'] = (df['Vowels'] / df['Consonents'])
➥.round(5)
#count the number of syllables in a word
def syllables(word):
  word = word.lower()
  if word.endswith('e'):
    word = word[:-1]
  count = len(re.findall('[aeiou]+', word))
  return count
df['syllables'] = df['domain'].apply(syllables)

#prediction code
from xgboost import XGBClassifier

pred = pd.DataFrame(df.data, columns = columns) # load the dataset
➥ as a pandas data frame
y = df.benign_dga # the binary target variable 1 for DGA 0 for
➥ benign. This was assigned in the data collection
#create training and testing sets
X_train, X_test, y_train, y_test = train_test_split(df, y,
➥ test_size=0.3)

#fit model
model = XGBClassifier(objective= 'binary:logistic')
model.fit(X_train, y_train)

#make predictions for test data
y_pred = model.predict(X_test)
predictions = [round(value) for value in y_pred]

# evaluate predictions
accuracy = accuracy_score(y_test, predictions)
print("Accuracy: %.2f%%" % (accuracy * 100.0))
```

A finely tuned model which predicts the likelihood of a domain being a DGA will serve your cybersecurity defenders well. It will save you time, energy and costs on detections. Example ML implementations of DGA detections include:

- Proxy requests for domains that look like DGAs
- DNS log detections for DGAs
- Emails with DGAs links
- Threat intelligence attribution of attackers matching DGA malware families

The ML DGA prediction accuracy mileage with the code above will vary. As is the case with every cyber defense detection, tuning or creating more features to be fed to the model can help increase accuracy. However, more features will add to the processing resources needed to generate a model. The process of building a machine learning model is a juggling act of trial-and-error. But so is cybersecurity defense.

Happy DGA hunting with machine learning.

RESPONSIBLE DISCLOSURE OF A MALWARE INFILTRATION ATTEMPT

by The Piano Guy

Lately I have noticed that the articles in *2600* are skewing towards the more advanced. In a way that is a good thing, because a decent percentage of the *2600* reader population can comprehend that, work with it, and use it well. At the same time, my perception is that there are still people who, like I did over 20 years ago, are just coming to the hacker community as non-experts interested in learning more.

Today I received a novel attempt to infect my computer (clearly they failed). Maybe it isn't novel to you, but it is the first time I've seen this. It occurred to me that a write-up on what happened, how I analyzed it, and how to act may be useful to the newer members of the readership. No huge revelations today, but useful to some. Also, the best way to respond (at least in my opinion) if something like this should happen again.

Last January I had a need to hire a contractor. There is a referral service in my local area, akin to Angie's List, but more honest because one can only get in by multiple positive referrals; buying a listing is not allowed. I picked a dozen vendors, sent out a blanket email to all of them with a link on Facebook to the work I wanted done explained well (to keep the email size down), and my phone number.

As an aside, I got very few responses, and none of them panned out. So that didn't work out so well.

Today (14 May 20), I received an email

quoting the body copy I sent out, with this direction.

The company I was sending to wasn't the one listed, the email didn't match that anyway, and I knew better than to click on the file attachment. That, and it was months late. At the same time, it was novel for a malicious actor to break into a company, look through their emails, quote their requests for quotes back to the customer that sent them, and then send them malware. That does increase the trust level a bit, and I can see some of our less informed friends and relatives say to themselves "well, it's not some random person, it's a response to an email I sent, and this is their answer."

Wanting to see more about what was going on, I opened up Authentic8 Silo, logged into my email, downloaded the attachment, and put it through Virus Total. No surprise what the results were.

While I think anyone reading this either already knew what virustotal.com was, or does now. Authentic8 Silo may be a different story. They provide a secure browser as a service, which lets a user surf the web without leaving a record, and with nothing being transferred to the local machine except pixels (unless seriously intentional choices are made). It's only $10 a month for an individual account and has some nice security features built in. I don't know if I get a spiff for referring people, but if I do I'll put an advert in the classified section next quarter with a referral code or

something. Of course, if you need it now, go get it and don't worry about me on this. You can't just buy it online; they have to talk to you first, but it's harmless. They are trying to assure that people are not using their service for malicious purposes. Authorized penetration testing is not considered malicious.

After I knew what I had here, I decided that I should let the people who had their computers infiltrated know. After all, they should let their customers know to not click on the link. Of course, I sent the same email out to a dozen companies, and if you look at what was sent back to me, it's not possible for me to tell who was hacked. So I sent out an email to everyone I wrote in January saying that they should check their computer systems to see if they have any sent emails to me today. Also, that even if they didn't, they should check their systems for infiltrations. In my email, I did provide a phone number to answer more questions, but I made it absolutely clear that I wasn't asking them to click on a link, I wasn't asking them for information, and that I wasn't looking to make them a cybersecurity client. By doing none of that (and loudly doing none of that), there was no way to infer an ulterior motive on my part, or for them to think that I was hacking them.

About a half hour later, I received an email from one of the companies telling me to "Replace the existing Noritz tankless water heater with a Navien tankless water heater. Install will include service valves and gas shut off valve to the unit. First responder discount given along with all other discounts. Code:20FRHW."

I was angry, as I was trying to help them and I got this as a response. I wrote back "DID YOU EVEN READ MY E-MAIL? You may have been hacked. I'm doing you a favor to tell you so, since I do cyber for a living. Sheesh!"

I got a reply with an apology telling me that they just sent me the wrong email, and that they were sending an email out to all of their customers saying *"Please do NOT open any attachments from Jim Workman and/or Dan McCarthy, we are working with IT to fix the issue. Sorry for any inconvenience."*

I replied with a thank you for the clarification, and realized that I had two more steps to take. I sent another email to everyone else I wrote earlier today letting them know that another company had acknowledged that they were the infected company (so they could stand down), and I knew I had to write this article.

Dev Manny, Information Technology Private Investigator "Hacking the Naked Princess"

by Andy Kaiser

Chapter 0x19

"You found the most boring font in the world. It's like Keebler green. What, you got a thing for AS/400s? You're weird, mate."

"Never said I wasn't."

P@nic pushed out a breath of concentration as her typing speed doubled. "I know a guy who's an AIX freak. There's a support group for people like you."

I hadn't bothered to turn on my office lights and neither had she. Her face was lit only by the sickly green glow of text scrolling by on her maximized Putty session. My PC was supposed to have a failsafe, but a hard knot growing in my stomach told me something was wrong.

"You've only got seconds left," I said. "The machine's got a dead man's switch. Since I haven't killed the timer, the drive and memory are about to be wiped clean. So while I hate to party poop on -"

"Oh right, you mean control-alt-shift-c? Within the first thirty seconds after OS load? That dead-man's switch?"

I stared back with a stone-faced expression that I assumed would be answer enough.

"Gotcha covered," she said. Nodding at something on the screen, she closed out whatever she'd been doing, then pushed away and leaned back. The display was empty now save for a lonely home directory prompt.

"Thanks for testing my security," I said, wondering how she'd gotten the information. She somehow snuck in a keylogger? Or was watching me work from a spycam somewhere? Radiating the best false confidence I could, I walked over to the wall and flicked on the light.

Reclining precariously in my rickety chair, she'd propped both feet on my filing cabinet. They thumped to the ground as she sat forward to point at the empty monitor.

"Just needed to shut down the botnet. Call off my armed forces. Update the blockchain for you." There was a faint smile that didn't reach her eyes. "RedAction's done."

"No, they're not." She watched bemused as I gestured behind me in a vague direction of the rest of the world. "I was just there. Or what used to be RedAction. They tore everything out of the office and ran."

Everything, except for the lone survivor of the exodus, a small USB drive that was weighing down my pocket heavier than the Panama Papers. Left at RedAction by an anonymous person, perhaps for me to find, for now I'd keep it to myself.

She was confused. "But we did it. Your infiltration. My botnet. I took out their servers. We shut them down."

"You think that's their only building? You think a place like that operates centralized? All they need is an IP on a new public subnet, and a little time."

"But -"

"Think about it. The fact that they disappeared so quickly is proof they'll be back."

Her face was sliding to pale.

"RedAction has been around," I said. "I don't know for how long, but it's been a while. In a month, the world will have one more new public IP, and they're back online. That's life. Just stay paranoid. Don't trust anyone."

She looked at me seriously. "Yeah, well, you can trust me. Thanks for your help. I owe you a lot."

"I'm just mad I let Reboot hire me to begin with, him posing as Oober with his fake mother. I should've seen it."

"You're not the only one he took in. I'm glad we exposed him."

"What are you going to do now?"

She tapped one finger against her lip for a moment. "I've heard that the darknets are beautiful this time of year. What about

you?"

I spread my hands to take in my tiny office. "This. It doesn't always pay the bills, but I like it." I shrugged, nodding at my PC. "Although since you've been playing with my toys, even though I of course absolutely trust you, something tells me I should sanitize that sucker. With a brick."

She waved her hands in surrender as she laughed. "Just give it a few more minutes before you do that. Let my transaction hit the blockchain. I'll help you pay those bills."

"Bitcoin?"

"Yup. It's down a lot. A little whale told me it's a great time to buy."

"A whale. A crypto whale?"

"I know someone. She likes to manipulate little things, like blockchain pressure and market demand. The last push she did got me a four hundred percent return." She swiveled around in my chair and looked up at me. "Wait five weeks before you sell any of it. That'll be the peak. Then do a quick trade to a stablecoin before it tanks again. Got it?"

I was already on my phone, looking at my bitcoin balance. What she'd given me the other day was plenty, but now... For the first time in my life I could measure my wealth in exponents. I looked again. My head felt a little light.

"Got it," I said.

She left. The second my door closed I went to my air gapped PC and the RedAction USB stick. It contained nothing but a text file. Apart from an uncomfortable reminder of the Naked Princess file, this one was nothing but two short number sequences. A position indicator? Latitude and longitude, maybe? Or a position relative to where RedAction had been? I wasn't sure, but I did know I had a new puzzle to chew on.

P@nic was gone. Wherever she went, I didn't hear from her again, but she'd told the truth about her whale of a friend. I ended up making a lot of money.

RedAction was still out there, somewhere, but without Reboot's manipulation, with P@nic off the grid, with the Naked Princess app growing more obsolete every day, RedAction seemed to have left me alone. As for the Naked Princess pictures, like everything else, they'd never disappear, but they were eclipsed by equally scummy parts of the Internet. They were nothing more than one small pool of brackish water in a very large swamp. Unless I wanted to dig through some very deep archives, I'd hoped to never hear about it again.

As for me, I enjoyed rolling around in my Satoshi-filled bathtub for a while. When she gave me the money, I didn't have the heart to tell P@nic I didn't really want it. I needed enough to live, but I couldn't be rich. It would blunt my edge. I saw the softness and weakness that came with too much money, and what I'd said to P@nic about not trusting anyone was also personal: I didn't trust myself to live rich. I didn't know how and would be fine without having to try.

While I kept a small amount as a safety net, someone in the Wikimedia Foundation's financing department had a very, very big surprise.

Money isn't enough. Money is the motivator for my body, but to get pseudo-religious, mystery and puzzles and excitement are motivators for my soul. And while, of course, my soul will eventually be consumed by Cthulhu in a bloody wave of cosmic destruction brought by the Great Old Ones, I still had some time left.

Until then, Information Technology Private Investigating kept calling, so I'd keep answering. Sometimes boring, other times exciting. Every once in a while I'd panic.

Just the way I liked it.

THE END

Thanks to 2600 *for working with me and the Dev Manny experiment. Thanks to you readers for being a part of this. If you want Dev to have more adventures, tell* 2600 *or you can email me your favorite yes/no equivalent at dev@andykaiser.com. -Andy*

HACKER HAPPENINGS

will return soon...

The first Cyberpunk Now Film Festival movie hackathon took place during Hackers on Planet Earth 2020.

After top secret required elements were revealed, participants had five days to produce and upload their short films. Thank you to everyone who participated, and major congratulations to the winners!

DRAMA AWARD
Cyber Boogie Shakedown
Cory McElrea and Krystal Pohaku

ANIMATION AWARD
Baud Zero Signifier
Aleksandar Bradic and Bogdan Rosu

EXPERIMENTAL AWARD
basicly-go-forth [sic]
Strick Yak and Cujo Bird

FOUND FOOTAGE AWARD
Cyberspace is where we..
Ben Combee

CYBERPUNK.HOPE.NET

Marketplace

For Sale

PORTABLE PENETRATOR. Find WPA WPA2 WPS WiFi Keys Pen Testing Software. Vulnerability Scanning & Assessment. Customize reports use for consulting. Coupon code 20% off: 2600. https://shop.secpoint.com

HACKER WAREHOUSE is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why we carry only the highest quality gear from the best brands in the industry. From RF Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Now including Offensive Security and Kali Linux branded merch! Check us out at https://HackerWarehouse.com.

OPEN SOURCE HARDWARE: crowdfunded and in-stock on Crowd Supply (crowdsupply.com). Includes software-defined radios (SDRs), DIY computers, NASs, FPGA boards, open silicon (RISC-V), hardware encryption/security devices, pentest tools, health monitors, kite-balloons, workbench tools, optical decoders, and opportunities to help fight the DMCA (see bunnie huang's NeTV2 project).

GUIDEBOOK TO COMPUTER AND SMARTPHONE SECURITY by Brandon of Lipani Technologies LLC has been released. This new security book can be purchased at https://leanpub.com/techgeek. Brandon is a certified CompTIA Security+ professional helping users and companies secure their computers, networks, and smartphones across the country. He says, "The purpose of this book is to educate and teach computer and smartphone users about safety and security online."

HEATHKIT BOOK: Interested in vintage electronics? *Classic Heathkit Electronic Test Equipment* by Jeff Tranter covers Heathkit's test equipment line, with in depth coverage of different models including oscilloscopes, meters, tube testers, etc., as well as a history of Heathkit and resources for collecting and restoration. 140 pages in 11 chapters plus appendices. Retails for $19.95 from lulu.com and amazon.com.

SECUREMAC.COM is offering popular anti-malware app MacScan 3 to help protect Mac users from malware, spyware, and ransomware. Download a 30-day trial directly from SecureMac.com. Looking for a new podcast? Check out *The Checklist* by SecureMac on iTunes, Pandora, and Spotify.

Help Wanted

VIRTUAL ASSISTANT/PROGRAMMER NEEDED. I have various tasks I need done but I am incarcerated. I will need both a programmer and a general assistant. Tasks include: 1) Internet research, 2) product ordering, 3) printing and mailing of documents, 4) some light programming tasks. Requirements include 1) printer, 2) webcam, 3) U.S. phone number, 4) Internet. No experience needed for assistant position but good Internet research skills a plus. Please send resume and salary requirements and contact me via phone when sent snail mail: 360-295-4317. Timothy Bach, 901 Port Ave., St. Helens, OR 97051

JOIN THE HTTPS://CODEFOR.CASH community and earn money with freelance programming jobs. All hats welcome!

PERSONAL ASSISTANT. I need someone to go online for me because I'm incarcerated and have no Internet access so I'm looking to hire a personal assistant. Pay: As agreed per project about 1-5 hours per month, you choose your hours. Duties: Internet research, Internet shopping, sending e-mail, etc. Must Have: Own phone, Internet access, computer and printer. Experience: No experience necessary but the following skills and interests are helpful. Self-motivated, the ability to follow instructions, and an attention to details. Computer and Internet skills. With an interest in the rehabilitation of criminals and the mentally ill, helping others, fundraising, and advertisement. Please mail me your name, contact address, and phone number, along with reason I should pick you. Eugene Banks, 1111 Highway 73. Moose Lake, MN 55767-9452

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Your feedback on the program is always welcome at oth@2600.com.

DON'T JUST CELEBRATE TECHNOLOGY, question its broad-reaching effects. 78 Reasonable Questions to Ask About Any Technology - tinyurl.com/questiontech

COVERTACTIONS.COM is the most comprehensive directory of encryption products anywhere. Search by type, hardware/software, country, open source, platform, and more. Now over 1036 products listed which include 221 VPN's, 192 messaging and 117 file encryption apps. These are just a few of the 28 categories available. There is no faster and easier way to find the encryption product that meets your requirements. Suggestions and feedback welcome. Now featuring news on important encryption issues.

TOG IS DUBLIN'S HACKERSPACE. We run regular events in coding, lock picking, electronics, craft, cad, wikipedia editing, electronic music, brewing, science fiction book club, and monthly socials. We recently celebrated our 11th birthday! TOG is run and funded by volunteer members and we are always looking for new hackers. website: www.tog.ie email: info@tog.ie address: 22 Blackpitts, Dublin 8, D08 P3K4, Ireland.

Services

DO YOU HAVE A LEAK OR A TIP that you want to share with *2600* securely? Now you can! *2600* is using SecureDrop for the submission of sensitive material - while preserving your anonymity. Anonymous tips and documentation are where many important news stories begin. With the SecureDrop system, your identity is kept secret from us, but we are able to communicate with you if you choose. It's simple to use: connect to our special .onion address using the Tor browser, attach any documents you want us to see, and hit "Submit Documents"! You can either walk away at that point or check back for a response using a special identification string that only you will see. For all the specifics, visit https://www.2600.com/securedrop (you can see this page from any browser). For more details on SecureDrop itself, visit https://securedrop.org. (SecureDrop was developed by Aaron Swartz, Kevin Poulsen, and James Dolan and is a part of the Freedom of the Press Foundation, used by journalists and sources worldwide.)

CALL INTO THE PHONE LOSERS OF AMERICA'S telephone network interface and hack into our collection of answering machines from the 80s, 90s, and 2000s. Listen to old episodes of Joybubble's "Stories and Stuff," old telephone recordings, adventure choosing games, and more! Dial 505-608-6123, 435-625-4232, or 845-470-0336.

LOCKPICKING101.COM is open to hackers wanting to learn physical security and the insides and out of locks and lock picking. Register to join one of the oldest Locksport communities online.

DIGITAL FORENSICS EXPERTS FOR CRIMINAL DEFENSE! Sensei's digital forensic examiners hold the prestigious CISSP, CCE, CEH, and EnCE certifications. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. We can recover data nationwide from many sources, including computers, external media, tablets, and smartphones. Sensei Enterprises believes in the Constitutional right to a zealous defense and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Sensei's principals have written 18 books on IT, cybersecurity, and digital forensics published by the American Bar Association. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703.359.0700 or email us at sensei@senseient.com.

BLACKSTONE LAW GROUP LLP. Unique among law firms, we have married the practice of law with the practice of information security. We are also the only law firm to offer bespoke threat intelligence. Designed to identify the hallmarks of impending cyberattacks (APT activity, phishing, credentials harvesting, etc.), with our own DNS monitoring and threat intel platform, OMNI, we have assisted hundreds of companies worldwide with the early detection, investigation, and termination of sophisticated cybersecurity threats before a breach or reputation damage occurs. Engineered for and by information security professionals, our DNS intel platform goes far beyond ordinary brand protection, safeguarding our clients full circle: from detection to takedown. Our lawyers have been the Chief Information Security Officer and Chief Compliance Officer of some of the world's most recognizable companies, have federal government experience in both intelligence and defense, and been partners in several Am Law 100 firms. At Blackstone Law Group, there is no lag time to "get the lawyers up to speed" on the technical issues surrounding an incident or investigation. Our combination of legal acumen and information security expertise results in great efficiencies that, by design, benefit our clients' bottom line. And perhaps most notably, one of our partners is Alex Urbelis who many readers will recognize from *Off The Hook*. Give us a ring or send Alex a note. We would be glad to speak to you confidentially about our threat intel and legal services. Blackstone Law Group LLP, alex@blackstone-law.com, 1201 Broadway, 9th Floor, New York, NY 10001, P: (212) 779 3070 x 101, https://blackstone-law.com.

DOUBLEHOP.ME VPN is actively searching for an acquisition partner that shares our vision (https://bit.ly/3a1bCuM). We're an edgy VPN startup aiming to rock the boat with double VPN hops and encrypted multi-datacenter interconnects. We enable clients to VPN to country A, and exit country B. Increase your privacy with multiple legal jurisdictions and leave your traditional VPN behind! We don't keep logs, so there's no way for us to cooperate with LEOs, even if we felt compelled to. We accept Bitcoin! Use promo code COSBYSWEATER2600 for 50 percent off. https://www.doublehop.me

UNIX SHELL ACCOUNTS WITH MORE VHOSTS. If you like funny, relevant vhosts for IRC, get a JEAH shell. You can also use vhost domains for email. Access new and classic *nix programs, compilers, and languages. JEAH.NET hosts bouncers, bots, IRCD, and websites. *2600* readers get free setup! BTW: Domains from FYNE.COM come with free DNS hosting and WHOIS privacy for $5.

ANTIQUE COMPUTERS. From Altos to Zorba and everything in between - Apple, Commodore, DEC, IBM, MITS, Xerox... vintagecomputer.net is full of classic computer hardware restoration information, links, tons of photos, video, document scans, and how-to articles. A place for preserving historical computers, maintaining working machines, running a library of hard-to-find documentation, magazines, SIG materials, BBS disks, manuals, and brochures from the 1950s through the early WWW era. http://www.vintagecomputer.net

DISCOUNT WEB HOSTING AND FREE WEB TRAINING. Squidix Web Hosting provides FREE WordPress training in Arlington, VA for Squidix customers. We provide fantastic web hosting for 1,000s of clients. We love our clients and they love us. Our ongoing *2600* promotion will give you 50% off any hosting service for the first year. This offer valid for any new accounts and includes a free CPanel transfer of one existing website. Sign up at www.squidix.com and use code 2600 on checkout.

HAVE YOU SEEN THE *2600* STORE? Plenty of features, hacker stuff, and all sorts of possibilities. We accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. EVERY YEAR of *2600* and EVERY HOPE TALK now available for digital download! Plus, we've lowered prices on much of our stock. Won't you pay us a visit? store.2600.com

Personals

WHAT'S UP, HC, I'm a single, aspiring hacker, programmer, coder, IT, computer engineer noob who is looking for real comradery and information on suggested reading/learning material. I've been inside for 10 years and therefore I'm way out the loop. I've been getting *2600* for about two years so I'm not all the way out the loop but I have 1000 questions. I'm looking for people to network, game, and research with. I have tech ideas I would like to create and collab on along with a woman who is intelligent and tech savvy as me. Brothers are encouraged to write me as well for I would like to only communicate and hang out with my Hacker Community. I'm from Houston, TX. I love to travel and read. All info is requested. If you have tips and suggested paths to learn code through books or your experience is well appreciated. I parole in two years. Even if you're just interested in picking up post-release, send me contact info. For what it's worth, I am also very good looking and fit with pictures. I'm not vain and only want those whose intelligence makes them feel as different as I do with an open mind. Reach me at Edward Lacy, TDC #1772002, 1697 FM 980, Huntsville, TX 77343 or Jpay.com or download the Jpay app and text/type a message to me.

PENPALS: Seeking people to write with interests in technology. I'm 30 and from Cleveland, Ohio, but currently incarcerated in rural Pennsylvania. We are on a quarantine lockdown and I'm bored to death. Before prison I worked network operations for an Internet service provider. Also worked at the Geek Squad for a short period. Being out of tech for so long, I'm feeling antiquated. There's no Internet here and hardly any resources to keep up. I have many other interests too, including sailing, general aviation, health/fitness, snowboarding, travel/foreign cultures, etc. I can share with you the many crazy stories of what really happens in prison. Use white paper and white envelope. NO address labels/stickers. It will be rejected and returned. Looking forward to your letters! Token, thanks for the shoutout in 37:1. Shoot me a letter sometime. Dan Nieberding, 61030-060, Federal Correctional Institution, PO Box 1000, Cresson, PA 16630, United States of America.

I AM A 35 YEARS YOUNG MALE that is currently incarcerated in a Texas state prison. I am seeking an open-minded, adventurous, and intelligent pen pal with an amazing hacker mindset to converse with. My interest includes science, deep space/the universe, traveling, sociology, and pretty much anything that I've never experienced. I am currently teaching myself Java, which I will admit is pretty difficult w/o a computer or an instructor, but I am making progress. My pastime reading includes *2600*, *Maximum PC*, *DuPont Registry of Fine Homes*, and the classic *Think and Grow Rich* by Napoleon Hill. If there are any women that would like to correspond especially about anything computer/tech-related, contact me. I will possibly be out around December 2020 or January 2021. My info is: Alfonso Solomon #1775876, 1391 FM 3328, Tennessee Colony, TX 75880.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. If you're an electronic subscriber, please send us a copy of your subscription receipt. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to marketplace@2600.com.

Deadline for next issue: 10/31/20.

WRITERS NEEDED!

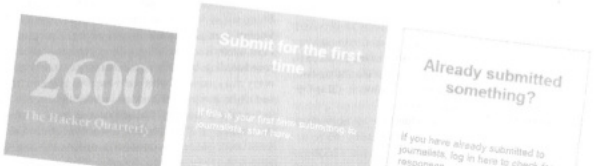
There are so many topics in the hacker world that capture our interest. And everyone reading this has their own story to tell involving technology and their adventures with it. We need more of you to send us those stories so we can keep capturing and inspiring the imagination of many readers to come!

Send your articles to us via email at **articles@2600.com**

We prefer ASCII but can read any format. Most articles are between 1000-2000 words, but we have many that are fewer and a bunch that are more. What's important is that you add your voice to those who have written for *2600* over the years. (We've never heard anyone say they've regretted it.)

For those without Internet access, our editorial department can be snail mailed at: **2600 Editorial, PO Box 99, Middle Island, NY 11953 USA**

All writers whose articles are printed will receive a one year subscription (or back issues) plus a t-shirt of their choice.



lxa4rh3xy2s7cvfy.onion

That is our SecureDrop address where you can submit leaks, tips, and files of all sorts while maintaining your complete anonymity.

Here's how it works. Get the Tor browser (www.torproject.org) if you're not already using it and go to that .onion address above. Attach any documents you want us to see, and hit "Submit Documents" and we will receive them without any identifying info. You can also send us a message and we can reply back to you, again without us knowing anything about you!

We've already gotten some really interesting material. Please consider adding to the pile! Voice recordings, videos, tax returns... well, you get the idea.

SecureDrop was developed by Aaron Swartz, Kevin Poulsen, and James Dolan and is a part of the Freedom of the Press Foundation, used by journalists and sources worldwide.

"Reality is that which, when you stop believing in it, doesn't go away" - Philip K. Dick

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
typ0

Cover
Dabu Ch'wald

Office Manager
Tampruf

S T A F F

Infrastructure
flyko

Network Operations
phiber, olssy

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Inspirational Music: Bright Eyes, Einstürzende Neubauten, Can
Shout Outs: Greenwood District, Wall of Moms, S.V. Dáte, the phenomenal HOPE 2020 crew, first responders, doctors, nurses, healthcare workers, scientists, and the USPS
RIP: Avi

***2600* is written by members of the global hacker community.**
You can be a part of this by sending your submissions to
articles@2600.com or the postal address below.

2600 (ISSN 0749-3851, USPS # 003-176) is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.

POSTMASTER:
Send address changes to: *2600*,
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. & Canada - $29 individual,
$50 corporate (U.S. Funds)
Overseas - $41 individual, $65 corporate

BACK ISSUES:
1984-1999 are $25 per year when available.
Individual issues for 1988-1999
are $6.25 each when available.
2000-2019 are $29 per year or $7.25 each.
Shipping added to overseas orders.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

MEETINGS

Due to the ongoing COVID-19 crisis, we are suspending all *2600* meetings until further notice. Even if numbers are good in your area, they can easily change very quickly and we don't want to do anything that could put any of our attendees at risk.

We know this is disappointing, but we will emerge from this period in history stronger and with renewed spirit. Please take this time to come up with new ideas for existing meetings and, if there's no meeting in your area, perhaps think of some locations to have them at. Please email us your ideas at meetings@2600.com.

We look forward to reconnecting in the near future. Stay safe!

Former Payphones

England. Found in Settle, North Yorkshire, this former phone booth is now used as a really tiny art gallery. (The postbox next to it still works.)

Photo by Mark

England. This combination was seen in Shenstone, Staffordshire and was sent to us mere days after the previous image. Of course, it's totally different, as this former booth is being used as a library. (And the postbox next to it still works.)

Photo by mike

United States. This art installation can be found in Point Reyes, California and is entitled "A Happy Heart is a Healthy Life." It was commissioned by the owner of the pharmacy behind it.

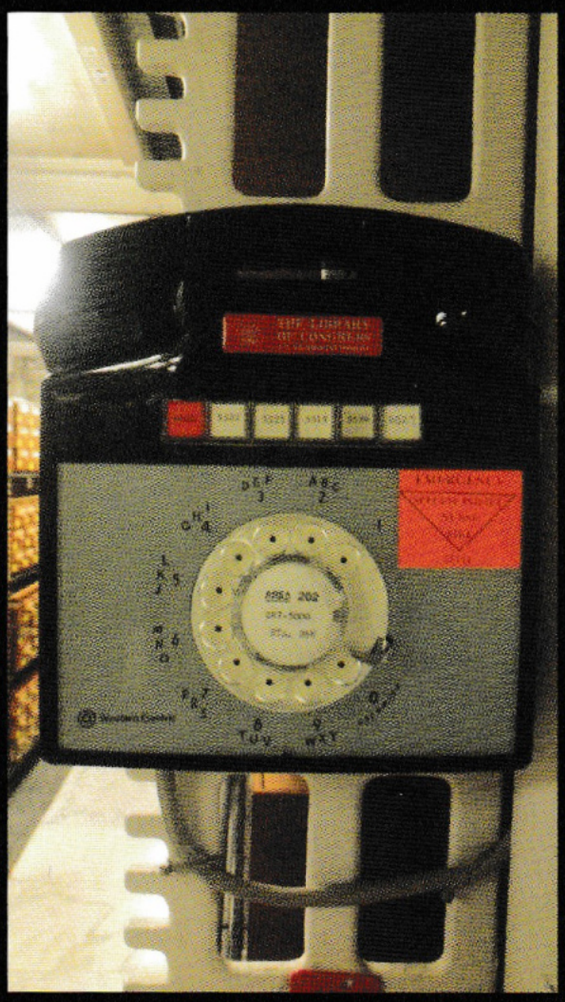
Photo by Peter

Canada. While it may no longer be a payphone, at least this is still a phone in Toronto. We're not sure how much people making distress calls will appreciate the surrounding artwork. We just hope the phone works.

Photo by Isoterric

Visit **www.2600.com/payphones** to see our foreign payphone photos!
(or turn to the inside front cover to see more right now)

The Back Cover Photos



Now how cool is this? The Library of Congress in Washington DC actually has this instrument on display in their archives room, which is usually not open to the public. Thanks to **Rafael Troncoso** for spotting this treasure, which apparently is still actively in use.

Attentive reader **sigflup synasloble** sent us an update on a picture we printed back in Autumn 2007 of this dive bar in Minneapolis with a magical number. We're sorry to see what happened to them during this year's riots. We're told they were on the corner of 26th Street and 26th Avenue. R.I.P.

If you've spotted something that has "2600" in it or anything else of interest to the hacker world (such as funny uses of "hacker," "unix," "404," you get the idea...), take a picture and send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed. Make sure and tell us where you spotted your subject along with any other info that makes it interesting - many photos are eliminated due to lack of detail.

Email your submissions to articles@2600.com or use snail mail to *2600* Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) and a *2600* t-shirt of your choice.